

Open Source Software in M&A and Finance Transactions

James G. Gatto and Hean L. Koo*

JUNE 5, 2018

Most, if not all, companies use open source software (OSS). Despite the ubiquitous use of OSS, not all companies effectively manage OSS legal risks. This can create legal issues for these companies. Often, these legal issues go undetected for some time. Typically, these issues surface as a result of diligence done in connection with financings, acquisitions or other corporate transactions. This is a very inopportune time to find out you have OSS legal issues.

If your company is looking to get acquired or funded, it is highly advisable to ensure that you have no OSS legal issues, *before* the acquirer or investor conducts diligence. Better yet, companies need to develop and enforce OSS policies to ensure that they have no unwanted OSS legal issues at any time. Companies can manage open source legal issues by developing and implementing an open source policy. An open source policy should provide written requirements/guidance on the approved uses of open source software for your company, and make sure that any use of open source is documented. Additional details on open source policies can be found in another article within this module, *Corporate Open Source Policies and Processes* [Open Source Software 600:100].

If your company is an acquirer or investor, and any software made or used by the target company is important to the value of the transaction, it is critical to conduct OSS diligence, assess open source legal risks and liabilities and ensure that the transaction documents effectively address the OSS issues.

This module addresses some of the potential legal issues with OSS software, how companies can manage OSS issues, the type of diligence that should be done in transactions, an overview of remedial actions and some key areas to cover in transaction documents. Each deal is different and an independent assessment needs to be made based on the facts. The following addresses some of the common issues that can arise, but is not necessarily a complete list of all issues.

1. POTENTIAL LEGAL ISSUES WITH OSS SOFTWARE

While the benefits of using OSS software are clear and well-known, there are significant legal risks that can arise from such usage.

- a. Tainting—In a worst case scenario, OSS legal issues can effectively prevent monetization of proprietary software that uses certain OSS. With some OSS licenses, any software that includes or is derived from the OSS code must be licensed under the terms of the OSS license. This can mean that recipients can freely copy, modify and redistribute the code. Additionally, the company may have an obligation to make the source code available to others. If the target company has software that it wants to license under a proprietary license, for a fee, this scenario creates a significant legal issue. This is often referred to as tainting of the proprietary software. This is one of the biggest potential issues in many transactions.
- b. Loss of License/Infringement—Most OSS licenses grant rights and impose obligations. If the target company has not been complying with the legal obligations associated with the OSS licenses they have been using, this can create legal issues. Some OSS licenses automatically terminate in the event of breach. In such cases, the target's software may be using OSS components for which it has no license. Its continued use of the OSS components, without a license, may constitute copyright infringement. Other liabilities for breach of contract may exist.
- c. Patent License Grants – many OSS licenses include patent license grant provisions. In some cases, certain usage of OSS by the target may subject it to granting patent licenses to others. The scope of these patent licenses can vary widely. If the target company has patents, which are part of the value of the transaction, it is critical to understand whether it is subject to such a patent license. If so, this can greatly impact the value of the patents.

These and other OSS issues need to be identified and addressed in any transaction, before the deal is done.

2. OSS DILIGENCE

OSS diligence requires identification of all OSS components used by the target company, the relevant licenses and the use cases. Based on that information, a legal assessment can be made to



determine if there are any significant OSS legal issues. The following is an overview of some of the key areas to focus on for OSS diligence.

- a. Does the target have a written OSS Policy? If so ask to review it, and ask how compliance with the policy is ensured. Many companies still do not have OSS policies. Often these companies have no idea what OSS is being used in or with its products and the associated legal issues it faces.
- b. OSS Components Used – it is imperative to determine all of the OSS components that are used by the target. In some cases, this information can be obtained by asking the question. Rarely, however, is the answer complete because many companies have no idea what OSS they are using. It is now common, when conducting OSS diligence, to use one of the commercially available tools to conduct a code scan, to programmatically determine all of the OSS components used in or with certain software. If you plan to do a code scan, do it early on the diligence process. It can take some time to do the scan and assess the results.
- c. OSS Licenses – for each of the OSS components identified, it is important to determine the governing license. This includes the OSS license and the version of that license. The license/version that governs is the one associated with the code that was downloaded by the targeted. Typically, this license information is included in a license file associated with the software.
- d. Use cases – it is important to understand how the OSS components are used because the obligations and issues that can arise with many OSS licenses vary by use case. Often, if an OSS component is used as a standalone tool, the issues are minimal. If the OSS is compiled with proprietary software, greater issues can arise. Many licenses have conditions that trigger when a licensee modifies the OSS component. Fewer issues arise when the OSS is used for internal purposes only. Greater issues can arise when the OSS is distributed. In general, it is important to understand:
 - i. how each OSS component is used (stand alone, library, linked to other software, compiled with other software, etc.);
 - ii. Whether the OSS component is used as is, modified or combined with other software; and
 - iii. Whether the OSS component is used internally, distributed or made available via network access (e.g., SaaS model).

b. Identify any OSS Legal Issues

Based on the information obtained from the diligence, a legal assessment can be conducted to determine if there are OSS legal issues. A list of common OSS legal issues can be found here: *Corporate Open Source Policies and Processes* [Open Source Software 600:100].

3. REMEDIATION OF OSS ISSUES

In some cases, if diligence reveals OSS legal issues, remedial actions can be taken. These can range from simple replacements of code to costly and time consuming rewrites of the code. In some cases, remedial actions may not even be feasible.

a. Remediation to avoid future issues where feasible

If feasible, have the target remediate OSS issues before closing. Remediation may include replacing problematic OSS components with other OSS code that is available under a more permissive license or by writing proprietary code to replace the functionality of the OSS component. Remediation may also include changing the way in which OSS is made available. In some cases, distributing an OSS component in certain ways with proprietary software can cause legal issues. To avoid this, in some cases, it may be possible to distribute the proprietary software and instruct the recipient to download the OSS component. Other remedial steps may be feasible depending on the facts.

b. Impact of past OSS issues

Remedial actions are often effective to prevent *future* OSS legal issues. Often they do not eliminate past liability. To the extent that any such prior OSS issues occurred, you need to be aware of them and determine how to deal with them. In an acquisition context, if you do an asset purchase (as opposed to acquiring the entity) you may be able to avoid assuming past liability. In some cases, prior breaches can be addressed by contacting the copyright owner of the OSS component to negotiate a mutually agreeable release and waiver of past liability.

4. OSS ISSUES TO COVER IN TRANSACTION DOCUMENTS

After conducting diligence and assessing the legal issues, it is necessary to effectively address OSS issues in the transaction documents. The following are some of the items commonly addressed. As always, each deal presents unique facts. Other issues may need to be addressed.

- Definition – this may sound obvious, but it is important to ensure that there is a clear and comprehensive definition of “OSS software.” Many agreements have an incomplete definition and refer to examples of OSS licenses.
- The transaction agreement should have an exhibit that lists the facts determined during the OSS diligence and include a representation by the target that the exhibit is an accurate and complete listing of the OSS used, the governing licenses and the use cases. Ideally, the representation covers not just the OSS used as of the closing date, but all prior use of OSS as well. This is important because even some prior OSS use may create OSS legal issues.
- Require the target to represent that it has not made, and is under no obligation to make, available the source code for any proprietary software.
- Require the target to represent that it has not used any OSS software in a way that requires it to grant a patent license to anyone.
- Require the target to represent that it had fully complied with all OSS license obligations, that it is not in breach of any OSS license, that none of the licenses used have been terminated.
- If any remedial actions are identified, include provisions in the agreement to specify the remedial actions that target must take and consider making that a closing condition.

This article first appeared in Westlaw’s publication entitled Open Source Software. The publication is part of the Emerging Areas of Practice Series – a new publishing initiative to cover emerging areas of law as they develop. New documents are loaded to Westlaw on a rolling basis as received and content is updated quarterly.

* © 2018, James G. Gatto and Hean L. Koo

ABOUT THE AUTHORS



James Gatto is a partner at Sheppard Mullin and is the leader of its Open Source Team. Jim has over 30 years of IP experience, with a strong focus on software, digital media and interactive entertainment. He routinely advises clients and delivers presentations on legal issues associated with open source software, including developing and implementing corporate policies on use of open source software, handling open source legal issues and diligence in transactions, open source patent issues, open source licensing business models and open source issues in the distribution chain.



Hean Koo is an associate at Sheppard Mullin and is the lead associate for its Open Source Team. Hean combines over ten years of IP experience and over five years of software development experience to understand legal and technical issues associated with open source software. He advises clients on developing and implementing corporate policies on use of open source software, handling open source legal issues and diligence in transactions, open source patent issues, open source licensing business models and open source issues in the distribution chain.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world’s most trusted news organization.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.