OSS Diligence for M&A - Best Practices

Authors:

Bob Ghosh, Avaya Inc.,
Theodore C. McCullough, Hewlett-Packard Corporation
Elaine K. Lee, Hewlett-Packard Corporation.

This paper was created by the authors for the Intellectual Property Owners Association Open Source Committee to provide background to IPO members. It should not be construed as providing legal advice or as representing the views of IPO.

OSS diligence for M&A - Best Practices

I. Why OSS Diligence for M & A is Important

Open Source Software (OSS) licenses[1] are ubiquitous in nature and have become a very common way to license software. Given this ubiquitous nature, OSS licenses may impact the valuation of Intellectual Property (IP) transferred during the course of a Merger or Acquisition (M & A) transaction. The classic example of how OSS may impact this valuation is by reducing the value of IP that was otherwise considered to be licensable under a proprietary license, but for its licensing under an OSS license. For the purpose of this whitepaper, we will be discussing the impact of the GNU General Public License (GPL)[2] on M & A transactions, and specifically the provision[3] of GPL that allows for the automatic licensing of downstream recipients of copyrighted technology licensed under GPL.

A. A Hypothetical

Imagine that ACME Corporation ("ACME") buys STARTUP Corporation ("STARTUP"), a maker of mobile device software. Part of this acquisition includes a Software Developer Kit (SDK) for developing mobile device tools. This SDK is the primary reason that that ACME bought STARTUP. Unbeknownst to ACME, the SDK includes the WebPro software library, a library that is licensed under GPLv2. The WebPro library was included in the SDK by a third-party vendor working with

---

[1] An open source license is a copyright license for computer software that makes the source code available under terms that allow for modification and redistribution without having to pay the original author. Such licenses may have additional restrictions such as a requirement to preserve the name of the authors and the copyright statement within the code. One popular (and sometimes considered normative) set of open source software licenses are those approved by the Open Source Initiative (OSI) based on their Open Source Definition (OSD). http://en.wikipedia.org/wiki/Open_source_license (last visited January 10, 2010). Some better known open source licenses include the GNU General Public License (GPL), the Mozilla Public License 1.1 (MPL), and the Artistic license. To date, only the terms of the Artistic license have been litigated in the U.S. *See* e.g., http://en.wikipedia.org/wiki/Jacobsen_v._Katzer (last visited on January 10, 2010).

[2] *See* http://www.fsf.org/licensing/licenses/gpl-3.0.html (last visited on January 10, 2010). *See generally* http://www.fsf.org/licensing/licenses/quick-guide-gplv3.html (last visited on January 10, 2010) (providing an overview of GPL version 3 (GPLv3) and comparing it to other GPL licenses such as GPL version 2 (GPLv2)).

[3] *See* http://www.fsf.org/licensing/licenses/gpl-3.0.html (last visited on January 10, 2010) (GPLv3 Section 10- "Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License. . . You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License. . . ") *See also*, http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt (last visited on January 10, 2010) (GPLv2 Section 1- "You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program."); (GPLv2 Section 2a- " b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.").

STARTUP. STARTUP is not aware of the inclusion of the WebPro software library in the SDK. Soon after the acquisition, it is discovered that neither ACME nor STARTUP have made the software source code available as required by the GPLv2.[4] The Software Freedom Law Center (SFLC), representing the author(s) of the WebPro library, brings suit to enforce the terms of the GPLv2.

The alleged violation of the GPLv2 by ACME underscores the complexities of performing due diligence in the M & A context when it comes to open source licenses. Specifically, the alleged GPLv2 violation was the result of the activities of a third-party vendor and not due to the activities of STARTUP, the acquired party. Any licensing due diligence performed by ACME would have had to extend beyond the code generated by STARTUP, to any code utilized by STARTUP in any proprietary product. Given the propensity by software developers to re-use code from a variety of sources, these complexities can grow exponentially. To address these complexities, a combination of identifying the licensing provenance of code, performing a technical analysis of the software code (code) and reviewing the compliance of each license should be employed when performing M & A due diligence of software code.[5]

II. Does target have a policy in place for OSS management?

When determining the provenance of code during an M & A due diligence, the acquiring company needs to determine whether the target company (i.e., the company being acquired) has a policy in place for OSS management and compliance. If a policy is not in place, this may affect the valuation associated with the target company's IP. Specifically, absent such a policy, additional warranties may be required if the target company is publically held, or a larger indemnity escrow, if the target is privately held.

A. How is OSS identified, tracked and approved for use?

The questions that counsel for the acquiring company should ask themselves are how is the OSS identified, tracked and approved for use and does the target have a proper inventory of this information. Put another way, what is the open source policy at the target company for identifying and tracking the use of OSS. The identification of this process may include determining one or more of the following.

---

[4] *See* http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt (last visited on April 2, 2011) (GPLv2 Section 3- "You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.").

[5] *See The Open Source Alternative: Understanding Risks and Leveraging Opportunities,* by Heather Meeker, pgs. 71-76 (discussing the use of provenance and objective, software based checking.)

1. Approval process

Assuming that the target company does have an open source policy, there must be an approval process that allows code to be submitted for review and approved for integrating or incorporating into a company's product. This process can include the involvement of a formal open source review board, or a specific compliance officer that approves code for distribution as OSS. The exact nature of the process can vary, with the key being that there is a documented process in place at the target company.

2. Inventory of OSS for each target product

Assuming there is a process in place for approving code to be released as OSS, there is more than likely some type of mechanism to be used to document the various submissions and approvals made to the above mentioned open source review board, or compliance officer. In some companies, this documentation may be in the form of a database linked to the website, where target company software developers may be able to make submissions of code that they would like to release as OSS. In still other companies, this documentation may be in the form of a repository of actual physical documents submitted by software developers to an open source review board or compliance officer.

3. Details of component use

Ideally, submissions should include the history (i.e., the provenance) of the code, how has it been used or modified, and what is included in the modifications. Further, the submission should shed some light on whether the code was an original work by the author, or a derivative work by the author. Clearly, it is the latter, derivative work case, that raises issues of OSS licensing compliance. If the code is a derivative work, then due diligence will need to be performed regarding the license terms under which the derivative work was created.

4. Compliance information

Compliance information should include details relating to steps engaged by the target to ensure that compliance with an OSS license has occurred. In some cases, this compliance may include a check list of completed steps or conditions of use that an open source review board or compliance officer will require in exchange for approval for use. The list may include a statement confirming that the software code that is covered by the OSS license has not been released in a proprietary product. Additionally, the compliance information may include date(s) on which the code was reviewed for compliance, and who performed the review.

5. Description of how each OSS component is used (modified, linked, distributed etc.)

Documentation regarding how each OSS component is used has relevance in the terms of understanding whether compliance with the terms of an open source license has occurred. For example, the GPLv2 license includes a linking exception that allows for an exception to the license terms to exist when the OSS is used in conjunction with (i.e., linked to)

other code in the form of libraries.[6] This documentation has value if a licensor of the OSS attempts to argue that the terms of the license were violated, as the documentation of the approval process can show that the licensor is incorrect in his/her assertion of a violation of the license terms. Further, such documentation can also be used to argue that a particular type of OSS is not a derivative work.

6. Software solution in place to help with tracking?

The tracking of the usage of OSS can be facilitated with a database that tracks such things as the OSS component name, component version, the source of the OSS, the license under which the OSS is licensed, derivative works generated from the OSS, and other critical information. This tracking can address issues of OSS provenance head-on by documenting the history of the OSS and its use.

7. Is there an OSS approval committee? Compliance officer? Are developers trained on OSS risks?

During the course of performing due diligence on the target, the representatives of the acquiring company should determine what type of mechanisms are in place to manage the risk associated with OSS usage. These mechanisms include the previously referenced committee (i.e., an open source review committee), and/or a compliance officer. Additional mechanisms may include a training regime that trains individual software developer on best practices in using OSS.

III. Identify target individuals who are involved in the OSS management process and have knowledge of OSS inventory

Within most targets there will be a specific individual or group of individuals charged with managing open source issues for a company. These individuals may be a senior level software engineer, attorney, or groups of software engineers and attorneys. Typically, some combination of software engineers and attorneys will be employed to identify the possible OSS code, how the OSS is being used and to determine licensing issues related to the same. The acquiring party needs to make sure it identifies such individuals and the relevant knowledge they may have regarding the target's OSS inventory.

IV. Does the target contribute to OSS projects? Do they have a policy for releasing code as OSS? What code have they released?

Central to OSS is the idea of contributing back to the OSS code base. For example, where GPLv2 is used as the license to distribute OSS, the source code for the OSS must be made available to the public as well as the object code. Often times, the source code is contributed back as part of an open source software project. These projects are often maintained on aggregation sites such as www.sourceforge.net and www.freshmeat.net.

[6] Compliance issues may also arise with respect to the use of, for example, the Limited-GPL (LGPL) and the correct use of (e.g., dynamic or statically linked libraries) code as part of a library. *See generally* http://en.wikipedia.org/wiki/GNU_Lesser_General_Public_License (last visited on January 25, 2010) (describing the uses of the LGPL in the linking context.).

Among other things, these projects help to manage code forking[7] and ensure that, per the OSS licensing requirements, the source code for the OSS is available to all who request it.

A target may have a policy in place for determining and documenting when OSS is to be released to an open source software project. The existence of such a policy may help in making a determination of whether the target company knew of the release of software as OSS, or whether the release was conducted outside of the guidelines of the policy (e.g., by a rouge actor). Further, OSS released to a project may be identified via versioning information maintained in a central code repository, and contained in the header of the OSS itself.[8]

V. Request details regarding compliance with OSS licenses

In addition to determining whether a target company has an OSS policy or mechanism in place to manage the risk associated with OSS usage, details relating to OSS compliance may be sought by the acquiring company. Specifically, a determination may need to be made by the acquiring company regarding the overall sophistication of the target company with respect to open source. For example, does the target company have a program in place to educate the rank-and-file employees as to open source compliance and how is this compliance managed? This becomes more of an issue, where software developers may obtain code that unbeknownst to them is licensed under an open source license, and is included in a proprietary product. Through asking such questions, the acquiring company is provided another way to ascertain the level of risk arising from OSS development as it relates to the target company's proprietary code base.

A. Target risk tolerance

If a target company is tolerant of the mingling of OSS and proprietary code, this tolerance can severely affect the value of the target company's IP if not managed properly. In the past, enforcement actions involving open source licenses were few due, in part, to the technical difficulty in ascertaining a non-compliant use of OSS. More recently, enforcement actions by SFLC and others have become more commonplace.[9] As a result, today there is a greater likelihood that risk tolerance by a target company could result in asset devaluation where the asset is proprietary code that is comingled with OSS.

---

[7] *See* http://en.wikipedia.org/wiki/Fork_(software_development) (last visited on January 10, 2010) (described as when developers take a copy of source code from one software package and start independent development on it, creating a distinct piece of software.).

[8] *See also* http://www.gnu.org/licenses/gpl-2.0.txt (last visited on January 10, 2010) (Section 2a stating "You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.").

[9] *See* http://www.softwarefreedom.org/news/2009/dec/14/busybox-gpl-lawsuit/ (last visited on January 10, 2010) (SFLC initiated suit against Best Buy, Samsung, Western Digital, JVC and other over alleged violations of the GPLv2 license).

B. Delivery of source code or offer of source

Some open source licenses, including GPLv2, require the delivery of source code or the making of the source code available to those who request it.[10] Various mechanisms may be employed to distribute the source code including the delivery of the source code with the product being distributed, or an offer to deliver the source code upon request. Failure to make the source code available could result in the termination of the license[11] and give rise to a copyright action by the licensors of the OSS. It was the failure on the part of ACME to make available the source code for the SDK that served as one of the basis for the initiation of the hypothetical lawsuit by the SFLC.

C. Attribution and pass through of licenses

Most open source licenses require attribution[12] to the original authors of the source code, and further for the license rights to pass to downstream[13] users of the source code. One source of risk for an acquiring company is where software developers for the target utilize software code from which they have removed the copyright notices, in effect plagiarizing the code from another source. Another concern is when a target company does not provide proper copyright attribution in its product documentation. This is especially problematic in that most open source licenses require some sort of attribution to the original authors of the source code, while not all open source licenses require the distribution of source code to downstream users.[14] Where attribution is not provided, the license may be terminated and the licensor may bring an action for copyright infringement. It may be prudent to have the target company identify this information in advance of the deal closing.

---

[10] *See* http://www.gnu.org/licenses/gpl-2.0.txt (last visited on January 10, 2010) (Section 3 describing the requirement that source code be made available to user of the OSS.).

[11] *See* http://www.gnu.org/licenses/gpl-2.0.txt (last visited on January 10, 2010) (Section 4- "Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.).

[12] *See* http://www.gnu.org/licenses/gpl-2.0.txt (last visited on January 10, 2010) (Section 1- "You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program."). *See also* http://en.wikipedia.org/wiki/Jacobsen_v._Katzer (last visited on January 10, 2010) (describing a cause of action for copyright infringement, where the defendant removed copyright notices and failed to properly give attribution to the plaintiff as the author of the code as required by the open source Artistic License.).

[13] *See* http://www.gnu.org/licenses/gpl-2.0.txt (last visited on January 10, 2010) (Section 6- "Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.").

[14] The Artistic License that is litigated in the *Katzer v. Jacobsen* case does not require the distribution source code under the terms of the license. *See* http://www.opensource.org/licenses/artistic-license-1.0.php (last visited on January 10, 2010).

D. Source Code Repository

As previously discussed under Section V.B, in many cases the terms of the open source license require that the source code for OSS must be made available to those who request it. A target may maintain a source code repository, if the OSS is central to the business of the target company. Given, however, the costs associated with maintaining a source code repository, a target company may rely upon one of the aforementioned aggregation sites such as www.sourceforge.net and www.freshmeat.net. Where the target company relies upon an aggregation site for compliance with the licensing terms, risk may depend upon the reputation of the aggregation site and/or whether the aggregation site is actually maintaining the source code repository.

E. Tracking of updates

Some OSS licenses require the tracking of updates in the form of modifications to the OSS.[15] Again, like the delivery of source code, and the need for attribution and licensing pass through, the failure to track updates can result in the terms of the license being violated. Where the terms of the license are violated, the license may be terminated and a suit for copyright infringement may be initiated.

VI. Target's tracking of OSS inventory typically is not accurate or doesn't contain sufficient information and most often there is significantly more OSS in the target product than identified

A major source of risk for an acquiring company is the difference between the stated and actual use of OSS by the target in the target's proprietary product. Depending on the type of open source license used, a use of OSS that exceeds the scope of the open source license can create copyright liability for the target and acquiring company. Acquiring companies need to be mindful of how otherwise trivial uses of code beyond the terms of the open source license, can create copyright liability. For example, some open source licenses allow for OSS to be dynamically linked to code that itself is not subject to the terms of the open source license covering the OSS. In some cases, however, where this code is statically linked to the OSS, the terms of the open source license apply with equal force to both the code and the OSS.[16] Accordingly, when performing due diligence, an acquiring company needs to have people on staff who understand the legal ramifications of otherwise minor uses or re-uses of OSS relative to the proprietary code use.

VII. Request target to scan source code base to verify or identify OSS

As referenced above, in addition to the use of the provenance of code, a technical analysis of the code can be employed to identify OSS. This technical analysis may employ the use of a software solution, or scanning tools to identify OSS. These tools can scan through source code determining whether the structure of the code is similar to known OSS.

---

[15] *See* http://www.gnu.org/licenses/gpl-2.0.txt (last visited on January 10, 2010) (Section 2.a-"You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.").

[16] *See* http://en.wikipedia.org/wiki/GNU_General_Public_License (last visited on January 10, 2010) (describing linking and derivative works).

A. Use third-party scanning tool (e.g. Black Duck, Palamida etc.) to assist in the evaluation of the target code base

Third-party scanning tools may be used to identify and perform a technical analysis of potential OSS code to determine whether the potential OSS code is actual OSS code. These scanning tools engage in code matching that compares the subject code against known OSS code that may exist in a third party vendor database. A report is generated showing potential matches that may be derivatives of OSS and the governing license associated with the identified OSS.[17]

B. Ensure to target that acquiring party will not get access to source code

To maintain the integrity of the technical analysis, the third party performing the technical analysis must appear neutral and in fact be neutral. Specifically, the third party must allow for precautions to not allow the acquiring company to gain access to the code once it is provided to the third party. Access by the acquiring company could result in the report being slanted towards the existence of a large number of positive results showing OSS being used in the proprietary offering of the target. Furthermore, a target will be extremely sensitive in ensuring that a third party doesn't release in what may be its crown jewel.

1. Request third party directly interact with target

The third party may also be used to solicit follow up information and interact directly with the target thereby further leveraging the third party's neutrality. Specifically, rather than the third party merely carrying out the directions of the acquiring company, in some case, it may be beneficial to have the third party directly contact the target for information. This preserves the appearance of neutrality of the third party, and shifts any dispute regarding whether code is OSS or not to the third party, and away from the acquiring company. Further, this shift assists in preserving the relationship between the acquiring company and the target.

2. Offer shared pricing option if too costly

Depending on the size of the project, the cost of retaining a firm to perform a technical analysis and scan of the code can be quite substantial. In such cases, this cost can be shared between parties. Further, if the requirement that such a code scan be performed is a contentious issue between the parties, a cost shifting regime could be implemented. This cost shifting regime may take the form of if any OSS is found as a result of the technical analysis, the cost could be shifted to the target from the acquiring company.

3. Pricing typically dependent on size of code base

The cost of a technical analysis in the form of a code scan typically depends on the size of the project (i.e., the amount of code to be scanned). Prices range anywhere from $15,000 to $50,000 depending on the size of the project, and can take 5 to 15 days to complete a project.

[17] It is worth noting that often times these same reports may be used to identify proprietary code. Once identified, the acquiring company can follow up with the target regarding the licenses covering the proprietary code.

4. Scan should highlight and identify licenses that are of concern to buyer

The results of a technical analysis and code scan should go beyond mere stating that code is in fact OSS, and should include a description of the open source license that the OSS being analyzed is purported to match. Absent such a description, the analysis is nearly worthless for the wide array of open source licenses require a variety of different steps for compliance. Moreover the acquiring company should inform a third party that is performing the scan the specific licenses it may be concerned with[18].

C. Make sure to request scan for code base of tangential products

It is better to be overly inclusive when conducting a technical analysis and scan of code for the purpose of determining whether the code is OSS. Code re-use is a very common practice in software development, and is in fact the rule rather than the exception. Given the prevalence of code re-use the potential that OSS could be used in tangentially related products is high. It is high because tangentially related products may share common functionality as included in libraries, or other statically or dynamically linked code.

D. Output - report of inventory of third party code – often has false positives

One problem with third party scanning tools is the result of false positives. Given the large amount of code that is associated with even the most trivial proprietary software product, a problem of false positives may arise. Specifically, code that is in actually proprietary in nature may appear like the OSS code that the proprietary code is being compared against. Moreover images of code used for the build but not remaining in the code typically can show up in results. The problem of false positives may be solved via the use of human reviewers to review the reported false positives to ensure that the false positives really are in fact false positives and not derivatives of OSS. It is also important to make sure the acquiring party has discussions with the target developers to confirm the scan results and understand exactly what may be a false positive.

1. Follow up with third party scan organization to cull and filter out false positives

The above referenced human reviewers can be supplied by the third party, the target company and by the acquiring company, or hired on a consultancy basis. Each of these options has its costs and benefits. Human reviewers supplied by the third party may have the advantage of being heavily experienced in the exercise of review, yet may have the disadvantage of being biased towards not recognizing the false positive so as to support the integrity of the software used to perform the technical analysis. Human reviewer supplied by the acquiring company may have the advantage of looking out for the interests of the acquiring company, but many acquiring companies may not have the expert experience on staff to perform such analysis. Human reviewers supplied by the target are often the best situated to identify what is actually in the code. Moreover they are able to go back and review the source code base to confirm any inconsistencies. A person hired on a consultancy basis may provide the best option for the acquiring

[18] For example, the acquiring company should specify the exact OSS licenses that are of concern (e.g., GPLv2, GPLv3 etc.).

company as such persons are often neutral in their review. One downside in using such a consultant is the cost associated with their use.

E. Follow up with target experts to discuss inventory identified in report and concerns

It is important to follow up with the target experts to discuss the results of the technical analysis and the scan results. Often times, the technical analysis may lead to a negative change in the valuation of the target company. It is important to discuss with the experts at the target the relationship between the results of the technical analysis and the changed valuation of the target. Further, such a discussion can assist the acquiring company in further understanding whether such a negative valuation is necessary. Also, by getting a chance to see all the licenses that are identified in the scan, the acquiring party can assess compliance obligations and inquire to see if these obligations have been met.

F. Discuss how each component is being used

One additional benefit of discussing with the experts at the target the results of the technical analysis, is that the experts of the target are given an opportunity to discuss how the use of OSS may be addressed so as to minimize the affect on the valuation of the target company. Specially, the experts of the target may be given the opportunity to discuss how a software component is being used such that it may be determined that the terms of the open source license are not applicable.

G. Discuss what can be removed and remedial measures if necessary

The expert of the target company may propose that the OSS code has been removed or can be removed so as to cure the problematic use of OSS. In some cases, OSS may be removed from proprietary code without substantive affecting the functionality of the proprietary code. Further, a design around may be implemented so as to replace the OSS with code that solves the same technical problem as the OSS, but in a matter that is not derivative of the OSS.

VIII. If target is in violation or not in compliance, see if problem can be mitigated

In cases where the target is not in compliance with the terms of the open source license, a number of remedial steps may be taken. These remedial steps include the removal of the OSS (i.e., the removal of the OSS component). A design around that is not derivative of the OSS may also be a potential solution. A solution to cure non-compliance may include getting the code into compliance. For instance, if attribution has not been provided, the acquiring party can ask the target to provide the missing attribution information.

A. Removal of component

As discussed above, it may be possible to remove OSS from a proprietary product and still have the base functionality of the proprietary product preserved. Often times, the core functionality of a proprietary product may be novel and unique, yet OSS may be used to augment this core functionality. This augmentation may be easily removed, or, as described below replaced.

B. Design around

Designing around is an option to cure the use of OSS. One problem with the design around is making sure that the design around solution is not a derivative of the OSS. The definition of what constitutes a derivative work is a matter of law and fact that requires the input an attorney.[19]

C. Assess cost to re-write code or bringing target product into compliance post closing

In some cases, the cost and time commitment of the design around makes it impractical to implement. Specifically, in cases where the OSS to be designed around makes up a substantial portion of the otherwise proprietary code, it may be impractical to perform a design around, or to otherwise re-write the code. In such a situation, the acquiring company should make a determination as to the how the existence of OSS negatively affects the value of the target.

D. Make sure individuals who have the most knowledge regarding the functionality have been identified

When determining whether the OSS code is part of a proprietary product, it is of critical importance that those individuals who coded the proprietary product are identified. Those individuals are best suited to be the ultimate arbiters of whether the code is proprietary or OSS as they can document the development process for the code at issue.

IX. Any letters, threats or allegations from third parties relating to OSS

As part of any due diligence process it is important that threats of litigation be disclosed by the target company. When it comes to OSS due diligence, the requirement that the threat of litigation be disclosed is no different. The threat of litigation over OSS may come in the form of a compliance letter from the SFLC.[20] The acquiring company should request that the target disclose all information in their possession relating to compliance and non-compliance assertions by third parties.

X. Any lawsuits relating to OSS

Law suits relating to open source licensing compliance are typically well publicized by those initiating the suits.[21] These cases are typically well publicized so as to put other potential violators on notice that violations of open source licenses are not without consequence. Due to the well publicized nature of these law suits there can be a public

---

[19] *See* e.g., *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 964 F.2d 965 (9th Cir. 1992) (performing a derivative work analysis with respect to software, ultimately finding no derivative work at issue). *See generally* 17 U.S.C.A. § 103 Subject Matter of Copyrights: Compilations and Derivative Works (West 2009) (describing derivative works); http://www.copyright.gov/circs/circ14.pdf (last visited on January 11, 2010) (providing examples of a what constitutes a derivative work according to the United States Copyright Office.).

[20] *See* http://www.softwarefreedom.org/news/2009/dec/14/busybox-gpl-lawsuit/ (last visited on January 11, 2010) (discussing the contacting of alleged open source license violators regarding compliance prior to the initiation of a suit for violating the terms of the open source license).

[21] *See* id. *See also*, http://news.cnet.com/8301-13580_3-9808378-39.html (last visited on January 11, 2010) (reporting the initiation of a law suit over open source license violations relating to busy box software).

relations fall out of which the acquiring company must be mindful. This public relations fall out may affect the ability of the acquiring company to realize revenue from the sale of goods and services marketed by the target company.

XI. Request reps and warranties from target re: OSS use, compliance and no adverse effects

In some cases, the acquiring company may request representations and warranties from the target company regarding OSS use. This is particularly the case where the target company is privately held, and the acquiring company has no public security filings upon which to rely. As previously discussed, based upon these representations and warranties, the acquiring company may request additional monies to be deposited into an indemnity escrow.

XII. Indemnification for breach of reps and warranties

As discussed above, indemnification can take the form of an indemnity escrow, or as will be discussed in more detail below insurance. An indemnity escrow typically will include 30-40% of the cost of merger or acquisition. However, the risk that is covered through the use of an indemnity escrow or insurance can be reduced if enough due diligence is performed at the front end of the M & A transaction. Specifically, known risks can be easily evaluated and a monetary value associated therewith determined. Unknown risks, however, are another issue especially where the existence of OSS in a proprietary product has the potential to substantially reduce the market value of the proprietary software.

A. Schedule scan report as exhibit to merger agreements

The results of a technical analysis in the form of a scan report may be affixed to the merger or acquisition agreement as a schedule or attachment. Such a schedule or attachment may be used to readily justify the terms of the merger or acquisition agreement.

1. No additional use of OSS post scan

Once the scan has detailed and identified the OSS found during M & A due diligence, the acquiring party should require the target to warrant that it has discontinued further use of OSS. This will ensure that no additional proprietary software is affected by the OSS, and the proprietary software that was previously cleared will not include any additional OSS other than what was disclosed by the technical analysis in the form of a code scan.

2. No distribution or release of OSS before acquisition is complete

No OSS code should be released before the acquisition of the target is completed. Such a release may create additional open source license based compliance liability for the target that may not be addressed during the due diligence process. This is especially true given the latency between the release of code and the initiation of a compliance action by the likes of the SFLC.

3. Seek insurance

Insurance indemnification can be used to reduce the risk posed by OSS to an acquiring company.[22] Such insurance, however, can be costly. As previously discussed, much of this cost can be avoided through an in depth due diligence performed up front.

XIII. If target refuses to agree on an audit, account for costs to have scans run as part of integration and adjust price to account for possibility of having to remove functionality and redesigning

As previously discussed, an indemnity escrow can be used to mitigate some of the risks associated with an acquisition. Specifically, if the target refuses to cooperate with an audit, the risk associated with the refusal can be built into the cost of the acquisition or calculated as part of the indemnity escrow. This cost can be related to the curing of the code to make it compliant with the open source license terms. Part of the cost may include, as previously discussed, the cost of redesigning, or removing the OSS code from the proprietary code base.

[22] *See* http://www.osriskmanagement.com/insurance.html (last visited on January 11, 2010) (describing the availability of insurance in the M & A context for acquisitions involving OSS.).

Checklist: OSS Diligence for M&A

☐ Does target have a policy in place for Open Source Software (OSS) management?

☐ How is OSS identified, tracked and approved for use?:

- ☐ Approval process
- ☐ Inventory of OSS for each target product
- ☐ Details of component use
- ☐ Compliance information
- ☐ Description of how each OSS component is used (i.e., modified, linked, distributed etc.)
- ☐ Software solution in place to help with tracking?
- ☐ Is there a committee? Compliance officer? Are developers trained on OSS risks?

☐ Identify target individuals who are involved in the OSS management process and have knowledge of OSS inventory

☐ Does the target contribute to OSS projects? Do they have a policy for releasing code as OSS? What code have they released?

☐ Request details regarding target compliance with OSS licenses:

- ☐ Target risk tolerance
- ☐ Attribution and pass through of licenses
- ☐ Source Code Repository
- ☐ Tracking of updates

☐ Request target to scan source code base to verify or identify OSS:

- ☐ Use third-party scanning tool (e.g. Black Duck, Palamida etc.) to assist in evaluation of target code base
- ☐ Ensure to target that acquiring party will not get access to source code:
  - ☐ Request third-party directly interact with target
  - ☐ Offer shared pricing option if too costly, pricing typically dependent on size of code base
- ☐ Scan should highlight and identify licenses that are of concern to buyer

- ☐ Make sure to request scan for code base of tangential products
- ☐ Output - report of inventory of third-party code – often has false positives:
  - ☐ Follow up with third-party scan organization to cull and filter out false positives
  - ☐ Follow up with target experts to discuss inventory identified in report and concerns
- ☐ Discuss how each component is being used
- ☐ Discuss what can be removed and remedial measures if necessary

☐ If target is in violation or not in compliance, see if problem can be mitigated:

- ☐ Removal of component
- ☐ Design around
- ☐ Assess cost to re-write code or bringing target product into compliance post closing
- ☐ Make sure individuals who have the most knowledge regarding the functionality have been identified

☐ Any letters, threats or allegations from third parties relating to OSS

☐ Any lawsuits relating to OSS

☐ Request reps and warranties from target re: OSS use, compliance and no adverse effects:

- ☐ Indemnification for breach of reps and warranties
- ☐ Schedule scan report as exhibit to merger agreements
- ☐ No additional use of OSS post scan
- ☐ No distribution or release of OSS before acquisition is complete
- ☐ Seek insurance

☐ If target refuses to agree on audit, account for costs to have scans run as part of integration and adjust price to account for possibility of having to remove functionality and redesigning