

Open Source Issues in Mergers & Acquisitions

By: Michael J. Cavaretta
January 06, 2015



In a merger or acquisition in which a technology company is the target, the target company's software is often a material – and perhaps even the principal – asset of the deal. Often, this software was developed using open source software ("OSS"). While there are several advantages to using OSS, including lower costs, potential quality improvements, and ease of use, a target's use of OSS to develop proprietary software products could also carry with it significant risks for the acquirer. Improper utilization of OSS could substantially reduce, or even eliminate altogether, the value to the acquirer of the target's software. Accordingly, it is imperative that a thorough and careful review of the target's use of OSS be conducted as part of the due diligence process.

This article will focus on two of the risks associated with a target company's use of OSS in the development of its proprietary software:¹ (1) the risk that the target company's software could have become "tainted" by the inclusion of OSS, causing the target company's proprietary software to itself become OSS; and (2) the risk that, under an OSS license, the acquirer would have to refrain from enforcing its patent rights in order to reap the value of the acquired software. This article will also briefly discuss the potential consequences associated with failing to comply with the terms of an OSS license.

Tainting Effect

Whether or not proprietary software developed using OSS is "tainted" by the OSS, and if so, to what degree, depends on the terms of the particular license under which the OSS was obtained.

OSS licenses generally fall into two categories – "permissive" licenses and "copyleft" licenses. Virtually all OSS licenses, whether permissive or copyleft, attempt to protect those who create or contribute to the OSS provided under the license ("contributors") from liability by including provisions disclaiming warranties and excluding liability.

The principal distinction between permissive and copyleft licenses is the effect of OSS use on a user's proprietary software. Permissive licenses permit recipients who use the OSS in or with their proprietary software to restrict other parties' access to the proprietary software. Examples of permissive licenses include the MIT License and the BSD licenses.

Copyleft licenses, by contrast, do not allow the same restrictions. Rather, these licenses impose "reciprocity" or "share-alike" requirements that require recipients who modify the OSS or develop proprietary software products that incorporate or combine with the OSS ("combined works") to make such modifications or combined works available to others under the terms of the same OSS license. The extent this "tainting" effect of the copyleft license has on the proprietary software created using the OSS depends on the "strength" of the copyleft license.

Under a "weak" copyleft license, a recipient must make the source code to any modifications it makes to the OSS available to others under the terms of the same OSS license. Examples of weak

copyleft licenses include the Mozilla Public License (MPL), the Eclipse Public License (EPL), the Common Development and Distribution License (CDDL), the Common Public License (CPL), and (under certain circumstances) the Lesser General Public License (LGPL).

Under a “strong” copyleft license, a recipient is required to make available the source code not just of modifications to the OSS, but of the entire combined work, and to allow others to freely modify and distribute the entire combined work. In other words, strong copyleft licenses cause an entire proprietary work which incorporates or is based on OSS to itself become OSS. For this reason, strong copyleft licenses are often referred to as “viral” licenses which have a “tainting” effect on proprietary software products if they incorporate OSS. The most prevalent example of a strong copyleft license is the GNU General Public License (GPL). Other examples include the Creative Commons Share-Alike License (CC-BY), the Berkeley DB License, and (under certain circumstances) the LGPL.

Under most copyleft licenses, the “reciprocity” or “share-alike” effects are only triggered when the software product containing the OSS is distributed (i.e., an actual copy of the product is made available) to others. However, under one strong copyleft license, the Affero General Public License (AGPL), the “reciprocity” or “share-alike requirements” are triggered not only if the software is distributed to others, but also if the software is provided on a hosted (i.e., software-as-a-service, or “SaaS”) basis.

Note that the LGPL may function as either a weak copyleft license or a strong copyleft license. If LGPL-licensed OSS is improperly combined with the recipient’s proprietary software, the LGPL could have the same viral or tainting effect as a strong copyleft license. Specifically, unlike most weak copyleft licenses, which allow OSS files to be linked statically (that is, directly copied into the otherwise proprietary software), in order to avoid tainting proprietary software under the LGPL, the LGPL-licensed OSS libraries must be dynamically linked with the proprietary software (that is, externally linked to from the proprietary software).

To point out the obvious, the tainting effect that strong copyleft licenses have on proprietary software is at odds with the objectives of most software license business models. The commercial viability of a software product so tainted could be significantly diminished, or even eliminated completely. To illustrate, when information technology conglomerate Cisco acquired the networking company Linksys, Cisco failed to discover that some Linksys software products contained OSS licensed under the GPL.² The Free Software Foundation (the “FSF”), which created the GPL, brought a copyright infringement action against Cisco. The FSF charged Cisco with violating the GPL for failing to disclose the source code of the Linksys software products it began distributing which contained GPL-licensed OSS.³ After reviewing its options, Cisco determined that it would be cost prohibitive to reengineer the software code and instead entered into a settlement agreement with the FSF, whereby Cisco agreed to release to the public the source code to the Linksys software products and allow its use, modification, and distribution under the terms of the GPL.⁴ As a result, Cisco was unexpectedly precluded from generating licensing revenue from the software products it acquired from Linksys.

Open Source Effect on Patent Enforcement

Included in many OSS licenses are express provisions that give downstream users the patent rights they need to use, modify, and redistribute the OSS without infringing the OSS contributors’ patents. These provisions may be phrased as the granting of a permission to practice a patent or as a covenant not to sue for patent infringement. In either case, the purpose of these provisions is to promote the innovation of modified versions of the OSS without future contributors needing to be concerned about the risk of being sued for patent infringement by other contributors whose patents cover some of the software.

Even if an OSS license does not expressly give downstream users requisite patent rights, these rights may be implied. A contributor’s conduct by otherwise giving downstream users permission under an OSS license to use, modify and redistribute the OSS could reasonably lead downstream

users to believe that they have been given the permission by the licensor to perform all of the steps needed to exercise such rights. Implied contracts may be afforded legal force.

These express or implied patent rights could be of major concern to acquirers who have a substantial patent portfolio that they wish to enforce. If an acquirer owns a patent that would be infringed by a third party's use of the target's software (absent a license from the acquirer), but that software contains OSS licensed with express or implied patent rights, the acquirer will be constrained in its options for licensing that software. The acquirer must choose between, on the one hand, not enforcing its patent, or, on the other hand, enforcing the patent and either modifying the OSS – which could be cost prohibitive; discontinuing the target software; or violating the OSS license – which could potentially expose the acquirer to the liabilities described below. Regardless of which path the acquirer chooses, such a situation could substantially reduce, or eliminate altogether, the commercial value to the acquirer of the target software.

Non-Compliance

As noted above, most OSS licenses – even permissive licenses – impose certain requirements on recipients of the OSS. These can range from obligations to display disclaimers, limitations of liability, and legal notices, to releasing the source code to proprietary works under the terms of the OSS license, to granting patent licenses. The potential liability for failing to comply with these requirements can vary from license to license.

The potential liability for non-compliance with the terms of an OSS license depend on whether a recipient's compliance with the agreement is a pre-condition to the effectiveness of the license for that recipient (as it is in the GPL and other copyleft licenses), or if the grant of license and the recipient's obligations under the license are independent covenants. If the recipient's compliance is a pre-condition to the effectiveness of the license, the potential exposure is much greater – in addition to having a cause of action for breach of contract upon a recipient's failure to adhere to the terms of the license, the OSS licensor could potentially bring an action for copyright, and perhaps even patent, infringement. This could entitle the licensor to significant remedies assessed against the recipient, including attorneys' fees, statutory damages (for copyright infringement), and treble damages (for patent infringement). If the grant of license and the recipient's obligations are separate covenants, the licensor may only be able to bring a cause of action for breach of contract upon a recipient's failure to adhere to the terms of the license.

Conclusion & Recommendations

Companies need to understand the potential risks related to acquiring a target that uses OSS in its proprietary products. Failure to identify issues in due diligence could lead to unexpected and undesirable outcomes for the acquirer, including having to release the source code to an acquired proprietary software product under a copyleft license, having to reengineer an acquired proprietary software product to eliminate the OSS, removing an acquired proprietary software product from the market altogether, and/or foregoing enforcement of certain patents.

Therefore, as part of its due diligence, an acquirer should conduct an audit of the target company's software code and development practices to discover red flags regarding risks, restrictions or obligations related to OSS software. The audit should at a minimum address the following questions:

- What target company products utilize OSS code?
- How is the OSS code incorporated into the target company's products?
- What OSS licenses apply to the incorporated OSS code?
- Are the affected products distributed or made available on a SaaS basis to others, or used solely for the internal operations of the target company?

- Is it commercially practicable to replace the OSS code with “closed” proprietary code, if necessary?
- What is the value of the products affected by OSS relative to the overall deal?

Conducting appropriate OSS due diligence will help potential acquirers avoid acquiring assets that could expose them to liability or restrict their ability to assert intellectual property rights against third parties, outcomes which could substantially reduce the value of the deal.

For more information, please contact **Michael J. Cavaretta**.

The author would like to acknowledge the contributions to this article by and give thanks to the following individuals: Emily Shaw, Northeastern University School of Law (NUSL) 2014; Evan Segal, NUSL 2015; and Jonathan Miller, NUSL 2015.

Check out our Top Merger Issues videos above!

Footnotes.

1 There are additional risks associated with the use of OSS, including those arising from the fact that most OSS is licensed “as is” and without warranty – in particular any warranty against intellectual property infringement – and the risk that because the target company did not itself develop the OSS, and may not even be aware of its origin or genesis, the OSS could contain unknown security vulnerabilities.

2 <http://www.fsf.org/news/2008-12-cisco-suit>

3 *Id.*

4 <https://www.fsf.org/news/2009-05-cisco-settlement.html>