# Open Source Issues in Mergers & Acquisitions

By:Michael J. Cavaretta
April 21, 2026



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 remains 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 focuses on two principal 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 proprietary software to itself become OSS, subject to OSS license obligations; and (2) the risk that, under certain OSS licenses, the acquirer's patent enforcement options, which are integral in an acquirer's ability to reap the value of the software that it acquired, may be constrained. This article also briefly discusses the potential consequences associated with failing to comply with the terms of an OSS license.

## What Is Open-Source Software?

In order to understand the risks and practices discussed in this article, one must first understand what constitutes "open-source software." Broadly speaking, OSS refers to computer programs that are freely accessible to the public, either as source code or object code, and are distributed under licenses that allow users to use, modify, and share the software with few restrictions. While such licenses may prove beneficial through their incentivization of collaboration and innovation, they too may prove burdensome as the legal obligations arising from such licenses may inhibit a user's ability to protect their creations, even those involving proprietary information.

## Potential Impacts of OSS on Proprietary Information

Whether proprietary software developed using OSS is "tainted," and 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 OSS in or with their

proprietary software to restrict other parties' access to the proprietary software. Examples include the MIT License, BSD licenses, and Apache License 2.0.

Copyleft licenses, by contrast, impose "reciprocity" or "share-alike" requirements that may 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 typically must make available the source code to any modifications made to the OSS. Examples of "weak" copyleft licenses include the Mozilla Public License (MPL), 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 may be 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" obligations are 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 made available over a hosted network, including software-as-a-service ("SaaS") deployments. As SaaS delivery models have become predominant, this distinction has become increasingly significant in technology transactions.

As alluded to above, 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.

## Effect on Patent Enforcement

Included in many OSS licenses are express provisions granting downstream users the patent rights necessary to use, modify, and redistribute the OSS. These provisions may be framed as patent licenses or covenants not to sue. In addition, certain licenses (including Apache 2.0) include patent retaliation provisions that, in efforts to deter litigation, may terminate rights if specified patent litigation is initiated.

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 (i) modifying the OSS – which could be cost prohibitive – (ii) discontinuing the target software, or (iii) 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.

## Emerging Challenges from Generative Artificial Intelligence

Since the original publication of this article, the increasing use of artificial intelligence systems has introduced additional complexity. AI products may incorporate OSS not only at the application layer, but also within model training code, model weights, and datasets. As such, there is a growing risk that targets may have, through their use of artificial intelligence, unintentionally tainted proprietary software with third-party or open-source code. Accordingly, it is essential that an acquirer's diligence efforts consider the target's AI Policy and the potential impact that it may have had on the development of proprietary information.

## Non-Compliance

Most OSS licenses – including 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, and 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 depends 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 and Recommendations

Companies must 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, including the obligation to disclose source code, the need to reengineer an acquired proprietary software product to eliminate the OSS, removal of an acquired proprietary software products, or limitations on patent enforcement.

As part of its due diligence, an acquirer should conduct an audit of the target company's software code and development practices to identify 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. However, further protection may be found through the incorporation of specific representations, warranties, and indemnities addressing OSS compliance.

## Conclusion

By making OSS diligence a central component of deal preparation and negotiation, both parties can reduce uncertainty, preserve deal value, and help promote a timely closing.

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; Jonathan Miller, NUSL 2015; Shayan Hedayat NUSL 2026; and Adam Sherf NUSL 2026.*

**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 ↩