synopsys®

WHITE PAPER

Open Source Software in SaaS Offerings: Truths, Myths, and Considerations

By: Anthony Decicco & Stephen Pakan, GTC Law Group & Affiliates
Phil Odence, Synopsys

Conservative investors or acquirers may require that your company have express hosting rights for all such third-party software. In addition, some code available online lacks a license altogether, and in those cases, unless a suitable license can be implied, use of the code should be avoided as all rights not granted are reserved to the author by default.

Technically, there may still be a distribution

Even though hosting is generally treated as separate from distribution, many SaaS offerings still distribute some of their code. For example, many SaaS offerings include a distributed mobile client front end (often available from an app store).

More subtly, many SaaS offerings use a server-client model that results in client-side code that is downloaded to, and executed on, a separate device (such as in a browser). This client-side code is often overlooked by "pure SaaS" companies that think their entire solution is hosted, which can lead to failure to comply with the relevant restrictions and obligations tied to distribution. Some common JavaScript components that run on the client side of products are licensed pursuant to the GPL (Sencha Ext JS, which is also available under a commercial license, is an example) and so care must be exercised with client-side components. There are few "pure SaaS" companies, so development organizations need to stay on top of which components are acceptable to use on the client side and which must be restricted to the back end. Knowing which components may be distributed is paramount to open source license compliance.

Patent termination clauses and patent right grant-back clauses

Many open source components are licensed under terms that do not require disclosing proprietary code that merely links with the open source component, but many of these licenses contain patent-related clauses. For example, the Microsoft Public License, Common Development and Distribution License, and similar "public" licenses (such as the Eclipse Public License and the Mozilla Public License) contain defensive patent termination clauses that may impact your ability to enforce your patent rights against the licensor, contributors to the open source project, and in some cases, other users of the open source project. Even if your company is using open source software in a SaaS offering, these types of patent issues may still need to be taken into account.

Security considerations

Security concerns related to open source software use

Particularly if your product is a SaaS solution, given its availability and accessibility, you need to know what open source components are in your code for security reasons. OWASP, the Open Web Application Security Project, is known for its list of Top 10 web application security risks. Number 6 is "Vulnerable and Outdated Components." It is widely known that, in 2017, Equifax's system was breached and may have resulted in the release of the personal information of over 143 million Americans. The source of the breach was traceable to an open source component, Apache Struts, that contained a security vulnerability for which a patch was available, but it had not been implemented by Equifax. The House Oversight Committee concluded in 2018 that Equifax's security practices and policies were sub-par and Equifax could have prevented the massive data breach. Regardless of whether Equifax could have avoided the breach by keeping up to date with Apache Struts patches, the point remains that, if you do not have a firm grasp on what open source components make up your SaaS product, you cannot keep up to date with ongoing security issues. In an investment and acquisition context, it is important to complete focused diligence in this area to avoid buying a breach and lawsuit.

Operational considerations

Respecting the spirit of open source licenses

A core principle of open source is attribution—don't use the code without giving credit to the authors. As a result, it is best to have a process in place to inventory the open source components on which you are relying, and that carries all the way through to providing notice and attribution. Since most common open source licenses were drafted before SaaS use was widespread, the attribution obligations are often triggered by distribution. Some SaaS companies take the position that their offerings involve no distribution, so they do not need to provide attribution, which may be seen as going against core open source principles. Even though the industry may have decided that certain usage patterns are exceptions to, or otherwise permitted by, some open source licenses, such exceptions or use may not be within the spirit of such licenses and may be viewed negatively by the open source community, potentially creating reputational and operational issues.

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.