Top Three Ways to Sabotage Your Licensing Compliance Under SPLA

By Christopher Barnett

Microsoft's Services Provider License Agreement (SPLA) is the principal licensing agreement for companies that want to use Microsoft products to deliver hosted software solutions over the Internet. Microsoft's standard volume license agreements expressly prohibit using the software for "commercial hosting" purposes (though, limited exceptions are offered for certain use cases and subject to specific requirements). SPLA offers an alternative licensing framework for companies whose hosting operations otherwise would be impeded by that prohibition.

All software licensing requires mature software asset management (SAM) practices to ensure that software usage does not exceed the scope of the entitlements acquired by a company. However, SPLA compliance entails special challenges, primarily because SPLA is based on a monthly license-reporting model. Instead of conducting an inventory and placing a forward-looking order for licenses to accommodate current and upcoming needs, companies licensing software under SPLA must confirm their usage each month and report that usage to an authorized SPLA reseller (such as Insight or SHI). In effect, SPLA licensees are required to conduct monthly, internal audits and to place monthly orders based on the results of those audits. Given that many companies lack the skill set required to conduct a single audit, the SPLA requirements can entail significant risks.

Most companies obviously want to stay in compliance with their contractual obligations. However, companies desiring to play chicken with the significant financial exposure that can arise under a SPLA audit initiated by Microsoft can magnify the extent of their non-compliance (and the payment required to settle the audit findings) by taking the following steps with regard to their hosting environments:

1. **Give Customers the Keys (and Don't Keep a Spare).** Many hosting customers want to limit the ability of service providers to access their IT environments. That is a natural inclination, especially for companies in highly regulated industries (such as healthcare or financial services), where applicable law imposes substantial data-security and data-privacy obligations. The fewer parties able to access a computing environment, the easier it is to satisfy those obligations.

   Hosting providers wanting to provide services to such companies often seek to accommodate that preference by setting up hosted servers on the providers' infrastructure and then surrendering all administrative access to those servers to the customers. However, providers subject to SPLA-reporting obligations take that approach at their significant peril.

   Without access, it is typically not possible to confirm what Microsoft products are being used within a hosted environment and, therefore, to accurately report what products are being "used" (more on that word in point 2, below). If the provider's customers have physically dedicated hosting environments, then it is easier for customers to provide their own licensing, thereby minimizing SPLA-reporting obligations. However, a physically dedicated hosting framework is not feasible or cost-effective for many companies, and hosting providers must be in a position to confirm all product usage within multi-tenant architectures.

1256 Main Street, Suite 200 · Southlake, Texas 76092
p 214.999.0080 · f 214.999.0333
Scott & Scott, LLP
Website · Disclaimer

Some companies that cede administrative access to their customers report usage under SPLA based on billing data and customer orders instead of up-to-date deployment inventories. This is a recipe for disaster. Over time, customers may add users or install additional or new Microsoft products in the hosted infrastructure. If those deployments are discovered during an audit, Microsoft's auditors will presume that ALL such usage is within the scope of the provider's SPLA obligations. If that provider has been reporting usage based on whatever a customer ordered when it signed its service agreement, then the gap between what is in use and what is reported (and the associated costs to resolve the audit findings) can be financially crippling.

The best approach is to retain administrative access to all hosted systems, to measure usage on a monthly basis, and to report usage based on those measurements. For companies that want to offer their customers an option where customers receive exclusive administrative control, it may be possible to configure the hosting environment to take advantage of technologies like Microsoft's "Shielded VM" functionality. (For more information on that option, click here.)

2. **Report Usage Based on Actual Usage.** No, really.

   Many companies make the mistake of reporting SPLA usage based on the number of users that actually access a product during a given month or on the number of servers actually accessed by those users. That's not an unreasonable approach at an intuitive level – use means use, right? – but under SPLA it is an incorrect approach that can yield significant compliance problems.

   SPLA requires that user-licensed products be licensed based on the number of users authorized to access a product, regardless of whether those authorized users actually access that product during a reporting month. Even if a company has reliable and accurate records to demonstrate actual user access, those records likely would be ignored by Microsoft's auditors during an audit. Furthermore, Microsoft defines the word "use" very expansively, to include the mere installation of a product on a server. Therefore, even if an installation in a hosting environment never has been run or used by an end user, unless the SPLA incorporates an explicit reporting exception that pertains to that installation, Microsoft auditors will assume that it must be reported.

   Companies licensing software under SPLA need to carefully review the agreement and to ensure that they understand all of the sometimes counter-intuitive licensing obligations that it incorporates.

3. **Save No Data.** Even companies that do a terrific job from month to month measuring product usage consistent with the SPLA's rules can face stiff compliance penalties if they save no records regarding the results of their monthly reviews. The SPLA typically is subject to a Microsoft Business and Services Agreement (MBSA), and the MBSA typically includes a recordkeeping requirement like the following:

   > "Customer must keep records relating to all use and distribution of Products by Customer and its Affiliates."

1256 Main Street, Suite 200 · Southlake, Texas 76092
p 214.999.0080 · f 214.999.0333
Scott & Scott, LLP
Website · Disclaimer

That is probably the single most overlooked contractual obligation among SPLA licensees, which may gather all of the information required to accurately report usage each month, but then promptly discard that information once the usage report has been transmitted to the reseller.

By itself, that oversight is not a source of compliance exposure. However, without data to demonstrate what a company's SPLA usage was during a historical month within the scope of an audit, the SPLA allows Microsoft to presume that any unreported use discovered during the audit began at the inception of the relevant end-user relationships, even if the deployments causing the compliance problems were installed within the past few months.

Therefore, we always recommend that our SPLA clients gather a complete set of inventory, Active Directory and virtualization data each month, in order prepare an accurate usage report, and then save those data in an archive, so that they may be retrieved and delivered to Microsoft's auditors, if necessary, during a SPLA audit.

SPLA – and Microsoft licensing in general – is full of pitfalls. Companies investing heavily in Microsoft's software products are well advised to tread carefully and to take steps to ensure that their procurement and SAM practices are consistent with their contractual obligations.

About the author Christopher Barnett:

Christopher represents clients in a variety of business, intellectual property and IT-related contexts, with matters involving trademark registration and enforcement, software and licensing disputes and litigation, and mergers, divestments and service transactions. Christopher's practice includes substantial attention to concerns faced by media & technology companies and to disputes involving new media, especially the fast-evolving content on the Internet.

Get in touch: **cbarnett@scottandscottllp.com** | 800.596.6176