

Compliance May Remain a Concern Even in the Cloud

By Christopher Barnett

For many businesses, the allure of moving their software platforms, applications and/or databases to The Cloud lies substantially in the promise of ridding themselves of license-compliance concerns. The [pitfalls](#) of a Cloud-based architecture are worth accepting for many businesses that do not want to expose themselves to the risks of hefty penalties or compliance purchases that may be required to resolve audits or other licensing disputes associated with having third-party software installed on their computers.

However, a recent report by BSA | The Software Alliance may indicate that while publishers' compliance programs may be undergoing some level of re-configuration in light of many companies' migration to The Cloud, they are not going away. In ["Navigating The Cloud: Why Software Asset Management is More Important Than Ever,"](#) the BSA identifies the following sources of potential licensing exposure for Cloud customers:

- Third-party IP infringement by the Cloud service provider
- Access to hosted services from unauthorized geographic regions
- Access to hosted services by more than one user via one account
- Access to hosted services by devices configured to appear as users
- Access to hosted services by non-employees
- Failure to use required plug-ins or utilities in connection with hosted services
- Failure to use required licensing metrics, especially in virtualized environments
- Improper use of "traditional" software licenses to support deployments in The Cloud

None of the above is very ground-breaking substantively. Most businesses that retreat to The Cloud to avoid license-compliance risks understand that such a move does not relieve them from all obligations associated with the delivery of hosted services. However, coming as it does from the "Software Police," the list provided in the BSA's report may give companies an indication of what to expect in the future from a "Cloud audit," if such a thing ever comes to pass.

More importantly, the list provides a good summary of some of the items that businesses need to address either internally or in their service contracts in making the move to The Cloud. Those contracts need to clearly define all of the company's obligations, so that any access-related restrictions may be monitored, and they also need to unambiguously assign the risk associated with third-party IP claims (preferably to the service provider).

As always, businesses considering any significant changes to their IT architectures need to carefully weigh the legal risks associated with those changes. Counsel should be involved in those decisions from the earliest stages in order to help ensure that the business is not simply trading one set of headaches for another.



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