It isn't all blue skies for cloud computing

Timothy J. Lockhart, Willcox Savage

As most businesspeople now know, cloud computing is the Internet-based system by which companies such as Amazon and Google with large hardware and software resources handle, process and store customers' data at multiple locations much as utility companies use a variety of resources to provide electricity over the power grid. Because of its significant benefits - comparatively low cost, rapid acquisition of capability and ease of expandability, among others - cloud computing is here to stay. But as with any new technology, significant practical problems give rise to legal issues.

Network World has compared the current state of cloud computing, with its fast growth and sketchy legal framework, to "a Wild West boom town." One major issue is the lack of data-security standards. This issue results partly from cloud providers' generally not being required to disclose where or how they store or process customers' data. The issue also stems partly from cloud providers' processing and storing data in countries that do not have privacy laws as strong as those in the United States and the European Union.

The Cloud Security Alliance, founded last year and having security-business members such as Iron Mountain and VeriSign, is now developing industry standards for the security of "cloud data." In the meantime, companies such as the online travel company Orbitz, which uses as well as provides cloud-computing services, is reportedly addressing the security issue by taking such due-diligence issues measures as conducting data-center inspections and on-site audits.

Other major issues include inappropriate or missing contract terms, inadequate warranties and indemnifications offered by cloud providers, and the currently unequal bargaining position between cloud providers and their customers. Some of these issues arise simply because relatively few lawyers have experience drafting, negotiating and interpreting cloud-computing agreements. Others arise because there is much less certainty about what should be the "standard" provisions for cloud agreements than is the case with more traditional types of software contacts.

Some cloud agreements, particularly those governing software as a service ("SaaS") evolved from earlier agreements used between application service providers ("ASPs") and their customers. Others evolved from outsourcing agreements or traditional software license agreements. But regardless of how they developed, cloud-computing agreements should provide a level of transparency about customers' rights, particularly with regard to their data.

Here are some important provisions to include:

- Agreements should contain performance standards, product warranties, intellectual-property ownership warranties and indemnification provisions similar to those in traditional software licenses.
- Customers should automatically get the benefit of a cloud provider's upgrades in hardware and software, not be locked into whatever systems the provider had as of the effective date of the agreement. For example, World Trademark Review reports that adding new features and functions quickly is one of the key vendor characteristics the U.S. Patent and Trademark Office is seeking as it moves toward "Trademark Next Generation," a cloud-based system for end-to-end processing of trademark matters.
- Agreements should cap cloud providers' fee increases at a certain percentage per year.

- Agreements should specify that cloud providers will give customers copies of their data on request and for a reasonable charge. Providers should not be allowed to keep data from their owners in the event of a dispute.
- Agreements should contain terms requiring cloud providers to cooperate with customers who become involved in litigation - for example, by helping to respond to discovery requests.
- Agreements should provide for a smooth transition period if a customer decides to move from one cloud provider to another.
- Agreements should permit customers to receive reasonable post-termination support from a cloud provider at the provider's customary hourly rates.
- Large customers should try to use their size as leverage to negotiate more favorable terms and conditions. The city of Los Angeles was reportedly able to do this with Google.

Likewise, because of the differences between cloud computing and traditional data processing, "cloud customers" should:

- Consider moving noncritical applications into the cloud first so that any transition problems will not be incurable.
- Pay attention to "geek" issues such as the need to have the right number of, and privileges for, system administrators and the possibility of using data encryption.
- Have cloud providers specify their data-backup policies, procedures and schedules.
- Require cloud providers to have written (and rehearsed) disaster-recovery plans - which, more broadly, all businesses should have, regardless of whether they use cloud computing.
- Not permit cloud providers to claim they have no liability for lost data - after all, they are responsible for hosting the data.
- Require cloud providers to state whether they own or control the relevant data centers or use other vendors' facilities. If they use other vendors' facilities, the providers should offer their customers a contractual remedy if those facilities fail for any reason.
- Require cloud providers to comply with all applicable export and privacy laws, including but not necessarily limited to U.S. laws. For example, the European Union Data Directive, which is generally more stringent than U.S. privacy laws, may apply in many cloud-computing scenarios.

Although there are a number of additional points, the foregoing list provides a general idea of why businesses should move cautiously when considering cloud computing. This new computing environment definitely offers many advantages. But only businesses alert to the sorts of issues described above can properly protect themselves if they decide to "enter the cloud."

Timothy J. Lockhart is head of the Intellectual Property Group at Willcox & Savage PC. He can be reached at 628-5582 and tlockhart@wilsav.com.