Legal and Quasi-Legal Issues in Cloud Computing Contracts

By Steve McDonald, General Counsel, Rhode Island School of Design

The following is a brief summary of the most common and significant legal issues that can arise in contracts with vendors for cloud computing services. Most of these issues are ultimately business ones, requiring business decisions, but they are "legal" in the sense that they either are embedded in the contract (typically in a way that favors the vendor) or *should* be dealt with in the contract (to ensure that the vendor's actions are appropriately constrained and that the vendor is accountable for its actions).

ISSUE	COMMENTS
FERPA (and privacy and confidentiality generally)	Much of our data—including student information databases and much faculty and staff e-mail—constitutes "education records" for purposes of FERPA and therefore may be outsourced only to vendors that we have designated, and that are willing to accept designation, as "school officials" with "legitimate educational interests" in the data. In order to do that, we must ensure both that our definitions of those two terms in our FERPA annual notices are broad enough to cover outsourcing and that the vendor will not use the data for any purpose other than providing the outsourced service (such as data mining for the vendor's own benefit) or redisclose it to others without appropriate authorization. There may be similar requirements under other statutes governing the privacy and confidentiality of specific types of information, and we are likely to want to protect the privacy and confidentiality of most of our data in any event. Any such requirements or desires should be set forth expressly in the contract, or they will not be enforceable. If the vendor is able to provide encryption of our data in both transmission and storage, privacy concerns, and the need for other contractual protections, may be lessened or even eliminated.
Data security	If they address the issue at all, vendor form contracts are likely to promise to provide only "reasonable" security for your data, or perhaps to adhere to "industry standard" security practices. While such promises sound good in the abstract, they are open to considerable interpretation and argument. It is preferable to specify an actual, specific, independent security standard and require that it be updated, and perhaps audited, regularly. In addition, for certain kinds of data (e.g., data subject to HIPAA, Gramm-Leach-Bliley, PCI DSS, or the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth), there may be specific security requirements that must be included in any vendor contracts. Ideally, the contract should also provide for regular SAS 70, Type II audits, with customer access to the results. Finally, the contract should require the vendor to give us notice of any security/data breaches, and, to the extent that user notification is legally required, such notice should preferably be in advance of user notification (which should be the vendor's responsibility).
Access to data for purposes of e-discovery	Although the contract probably will not (and probably need not) expressly address the issue, it is important to understand—ahead of time—the architecture of the vendor's system, how and in what format it keeps your data, and what tools are available to you to access your data so that you will be ready for any e-discovery needs that may arise. "Free" services typically will have few such tools available, which likely will make e-discovery a time-consuming and cumbersome task.

Location of data	Some vendor form contracts expressly reserve the right to store customer data in any country in which they do business. Others may not address the issue, but the vendors may follow similar practices nevertheless, on the (generally legitimate) theory that what is not expressly prohibited is thereby permitted. While dispersed geographical storage is beneficial from a data protection and backup perspective, it can raise export control (EAR/ITAR) issues in the context of research data. If that is important to you, you should be sure to include language prohibiting "extraterritorial" storage.
Responsibility for end users	Vendor form contracts sometimes require us to "ensure" that any end users comply with the vendor's AUP, terms of service, or similar provisions, or (better, though still problematic) to use "best efforts" or "commercially reasonable" efforts to do so. That may be appropriate with respect to faculty and staff, for whom we can be vicariously liable, but it is preferable to provide simply that we will "inform" our students, for whom we are not vicariously liable and over whom we have little control, of their obligation to do so. An alternative, and better yet, would be to provide that the vendor may require student end users to agree directly with the vendor to comply with any such provisions.
Unauthorized or inappropriate use	Vendor form contracts may attempt to make us responsible for affirmatively preventing any "unauthorized" or "inappropriate" use of the vendor's service by others, or perhaps to use "best efforts" or "commercially reasonable efforts" to do so. Given that these services are "in the cloud" and therefore largely outside our control, it is preferable to provide only that we will not "authorize" or "knowingly allow" such uses. Such contracts also may require us to notify the vendor of "all" unauthorized or inappropriate uses of which we become aware. Particularly with respect to vendors with broadly stated AUPs or terms of service, such expansive obligations seem burdensome and unnecessary. It is preferable to replace "all" with "material" or some similar, higher threshold.
Suspension of end-user accounts	E-mail services in particular may wish to retain the right to suspend your end users for violations of the vendor's AUP or terms of service. If, as is common, those provisions are broadly stated, the vendor will have almost open-ended authority to suspend your users. It is preferable to limit any such power to a more restrictive standard—perhaps only "material" violations, or violations that "significantly" threaten the security or integrity of the vendor's system.
Emergency security issues	Vendors understandably may wish to have the right to "immediately" suspend an "offending use," and possibly the service altogether, in the event of an "emergency" issue. However, the standard for what constitutes an emergency should be clearly defined, should not give the vendor much if any discretion or flexibility in its application, and, preferably, should incorporate a "materiality" or similar threshold.
Suspension and termination of the service	Vendor form contracts typically give the vendor the right to suspend the service or to terminate it altogether upon certain events or conditions. Such provisions are not unreasonable in the abstract, but they should be limited in scope to only truly significant matters, provide for an opportunity for you to cure the alleged violations or some form of escalation rather than instantaneous implementation (except in the case of true emergencies), and give you adequate time to make alternative arrangements for your data or service. (In the case of an e-mail system, it may take 6 months or more to establish and transition to a new system, particularly if you intend to completely dismantle your internal system once you outsource.) It also will be important to have assurance your data will continue to be available to you, in a usable format, for at least that long (or, if the vendor is unwilling to commit to a specific length, a "commercially reasonable" period of time) following any termination, as well as that the vendor will return or destroy any copies of your data once transition is complete.

Ownership of data	The contract should expressly make clear that all data belongs to the institution (and/or its users) and that the vendor acquires no rights or licenses, including without limitation intellectual property rights or licenses, to use the data for its own purposes by virtue of the transaction. It also may be useful to provide that the vendor does not acquire and may not claim any security interest in your data.
Publicity	Vendor form contracts sometimes grant the vendor the right to use customer names, logos, and trademarks for purposes of the vendor's own publicity. If such provisions (which are of no benefit to us) cannot be stricken altogether, they should be modified to require prior review and approval (perhaps "which may not unreasonably be withheld"), or at least limit use to the inclusion of our names (but not logos or trademarks) on a customer list, in a manner that does not state or imply an endorsement.
Service level agreements	The amount of guaranteed "uptime," the process and timeline for dealing with "downtime," and the consequences for any failures to meet those requirements should be spelled out clearly. In the context of a "free" service, additional "free" service is of no great benefit to us, and no great disincentive to the vendor.
Disclaimer of warranty	Vendor form contracts typically disclaim essentially all warranties, sometimes expressly including any warranty that the vendor's service does not infringe third-party intellectual property rights. At a minimum, the contract should warrant that the service conforms to and will perform in accordance with its specifications (which should themselves be as detailed as possible, to avoid misunderstandings and disagreements) and that it does *not* infringe any third-party intellectual property rights. Without those two warranties, there is no enforceable assurance that the service will in fact do what the vendor's marketing people claim it will do or that the vendor even has the right to provide it to us—and, if it doesn't work, or if we are sued for infringement, we will have no recourse against the vendor.
Indemnification by customer	Some vendor form contracts require us to indemnify the vendor not only for our own actions (which is not necessarily unreasonable), but also those of our end users, including students for whom we are not otherwise vicariously liable. With respect to liability for student e-mail, online postings, and the like, this is largely an issue of who will pay the vendor's attorney fees, as the vendor has good legal defenses against claims based on end-user content or actions. Moreover, this is not really taking on a new liability, as we currently can be sued for such content or actions (and have the same legal defenses) as ISPs ourselves. Nevertheless, it is preferable not to voluntarily accept that liability, which is also no different that the vendor's liability for any other, noninstitutional end users. Public institutions may also have significant state-law restrictions on their ability to indemnify.
Indemnification by vendor	Vendor form contracts rarely include any form of indemnification benefitting us, but such protection is critical in at least two areas: infringement of third-party intellectual property rights and inappropriate disclosure or data breach, both of which are largely, if not entirely, in the vendor's sole control, and both of which can be extremely costly to defend and remedy. (If, as has happened, a vendor refuses to accept liability for either of these issues on the ground that it's a "black hole," we should take that as a great warning about the vendor's lack of confidence in its own service and look elsewhere—what the vendor is really saying is that it expects *us* to be its insurance company.) Ideally, the vendor would indemnify us for all of its acts and omissions.

Modifications to the contract	Vendor form contracts sometimes reserve the right for the vendor to make modifications to its services unilaterally. While some form of right to make changes probably is necessary and appropriate—we certainly would have no objection to improvements—such language is overbroad and does not provide the customer with any assurance that any such modifications will be beneficial, let alone acceptable. Limiting the vendor's right to "commercially reasonable modifications" would be an improvement, but, in the context of a "free" service, could still be expansive. Even better would be to add to that a qualification prohibiting "materially detrimental" modifications—perhaps something to the effect of "Vendor may make commercially reasonable modifications to the Service, provided that they do not materially diminish the nature, scope, or quality of the Service."
Incorporation of URL terms	Similarly, vendor form contracts may incorporate by reference additional terms and policies posted to the vendor's website, which typically are subject to the vendor's unilateral amendment, and those terms and policies may in turn incorporate by reference still other terms and policies posted elsewhere on the vendor's websites, which also typically are subject to the vendor's unilateral amendment. The result is that the contract itself is incomplete, it may well contain provisions that are inconsistent or that conflict with the incorporated provisions, and it likely will be difficult or impossible to fully comprehend. It also will potentially be meaningless, because the vendor will have the right to amend it significantly at any time, and likely even without any more notice to us than posting the change to its website. While it may be reasonable to deal with technical standards and guidelines or other "non-legal" matters elsewhere, it is strongly preferable that all contractual terms be included in the contract itself. At the very least, the customer should attempt to require the vendor to provide direct, individual notice sufficiently in advance of the effective date of any amendments to incorporated terms, along with the right to terminate if such amendments are unacceptable or materially detrimental to the customer's interests.
Automatic renewal	Vendor form contracts typically renew automatically for additional terms unless we give specified prior notice. This is probably not a major concern in the context of "free" services, assuming there is nothing in the contract that actually requires us to use the service (particularly exclusively); we can simply cease to use it, with no significant adverse consequence. In other cases, however, it will be important to use a "tickler" system to remind us when we need to make a decision about renewal and give notice of any termination. Ideally, the contract would renew automatically (so we don't have to renegotiate every time), but also allow termination for convenience on some reasonably short period of notice.
Governing law and jurisdiction	Almost certainly, a vendor's form contract will specify that it is governed by the law of the vendor's home state and grant the courts of that state exclusive jurisdiction over any disputes arising out of the contract. Public institutions generally have significant state-law restrictions on their ability to consent to such provisions, and they are inadvisable for others. It is preferable to either (a) specify the law and jurisdiction of our own state (large vendors likely operate in and are subject to all such jurisdictions, so it is no significant inconvenience for them), (b) provide that disputes must be brought in the defendant's jurisdiction (which is even-handed and tends to encourage informal resolution, as the plaintiff won't have the "home court" advantage), or (c) simply delete the provision and leave the question open for later argument and resolution if and when needed.