

# From Users to Choosers: The Cloud and the Changing Shape of Enterprise Authority

*Ronald Yanosky*

For a long time, people working in IT have been accustomed to describing those they serve as users. It's an unsentimental term that suggests a division between those who merely *use* computers and those who make the magic happen—the ones who are really in control. The term is a lingering reminder of the days when computers were rare, housed in glorious isolation, and tended by professional staffs whose main focus was keeping the machine running, preferably at a healthy distance from the users. And keeping it running was critical: The organization that owned the machine often owned the institution's whole computing environment.

Granted, it's been a long time since that state of affairs prevailed. But even though the central IT organization's monopoly on computing resources has dissolved into messy complexity, a potent legacy remains: what might be called central IT's "enterprise authority," that is, the responsibility (and often, at least, the power) to define computing norms that protect the interests of the enterprise, and thus the interests of the user community as a whole.

The origins of this authority lie in the era of technological scarcity. When higher education IT administrators controlled most or all of the cycles and programming skills available, they effectively had the power to allocate computing itself. Computing at higher education institutions might be divided between administrative and academic units, each with its own mainframe, but each of these served large and diverse communities that crossed departmental boundaries. Over time, IT administrators had to develop new skills beyond the care and feeding of the technology: understanding the requirements of users who often could not articulate their own technical needs; determining priorities, allocations, and funding models; and, critically, arbitrating among departments that competed for IT resources but rarely communicated with each other.

This king-of-the-hill position made IT units uniquely conscious of how different uses of computing were related. Their domination of programming skill also gave IT units growing influence over business and academic operations on campus. Business rules and enterprise controls were increasingly embedded in the applications that IT developers built, and because they had to make different applications work together, the developers often came to understand overarching enterprise issues better than the functional departments themselves. This, in turn, gave them a degree of ownership over enterprise controls. All this, of course, was deeply disturbing to users who were accustomed to a high degree of operational autonomy.

Minicomputers, PCs, and the Internet eroded IT's direct control over cycles and programming skills, yet at the same time they fed the need for an ever more refined and complex exercise of enterprise authority. Users exulting in their liberation from the cycle gatekeepers in IT soon discovered that they had inherited system administration tasks that either sent them back to the IT organization asking for support or forced them to develop their own IT skills and sensibilities. And as soon as they tried to connect their departmental and personal machines to resources outside their immediate domain, the newly empowered users found themselves dependent on a central IT connectivity monopoly and tangled up in inter-departmental politics in which central IT played the role of arbiter.

## **The Federal Model**

By the time of the client-server era, this mix of new capabilities and new dependencies had shaped higher education's user-IT relations into a roughly "federal" model. Users had, in fact, broken free from many of the constraints of the data processing era. PCs put computing power on the desktop, and the new platforms and applications on them had helped create a popular user group culture in which participants could sharpen their skills and discover their common interests. Increasingly, even people who weren't technically adept began to identify themselves by their technologies of choice. The user group culture often had a libertarian ideology that prefigured later web-based cyberculture, yet its anti-institutional impulses were to some degree curbed by user reliance on departmental, school, and enterprise resources.

Above the "citizen" layer of individual users stood the "local" and "state" layers of the federal IT hierarchy. At large institutions, departments and schools began to develop their own IT organizations, ranging from small local-area networks (LANs) in offices or labs to big, ambitious data centers in computing intensive areas. Likewise, more and more of

the functional work of administrative (and some academic) departments migrated from manual to automated systems. In contrast to the more freewheeling nature of the popular user groups, these users came together along organizational lines, some concerned with specialized or cross-cutting computing needs, such as research support, and others representing slices of enterprise functions, such as the line business units and the registrar's office. As these users became more numerous, savvy, and familiar with technology, their political influence grew correspondingly.

Yet central IT was not completely shut out from the big decisions affecting these constituents. A degree of technical dependence remained, increasingly focused on network and support issues, but central IT's enterprise authority was the really dynamic element in preserving its influence in user relations. Central IT's administrative applications development skills remained important, and with the advent of integrated enterprise resource planning (ERP) systems, IT shifted from being an automater of business systems to an integrator and process designer, accentuating its pan-institutional profile. After some painful lessons, central IT units learned to shun the perception that they "owned" ERP projects. Yet even as they shared power with user departments, they remained a sort of first among equals, and often the most energetic advocates of business process change, in the project and IT steering committees that oversaw these initiatives.

Furthermore, central IT remained in the driver's seat of the revolutionary new network technologies and other crucial aspects of the computing infrastructure. It controlled the increasingly essential network backbone and negotiated most of the wide-area network (WAN), telecommunications, and Internet connectivity contracts that governed the institutional network environment. It also operated the "big iron" servers that increasingly absorbed old mainframe workloads, and had backup and disaster recovery capabilities unmatched elsewhere on campus.

These powers reinforced central IT's role managing the growing interconnections that now typified campus computing. Executive leaders reflexively looked to their CIOs for solutions and policy recommendations for any problem remotely connected to technology, from implementing telecommuting programs to disciplining students who sent malicious e-mails, and this growing executive concern gave the CIO's office political weight. Central IT was far from a technology autocracy, but it had a set of carrots and sticks at hand that no other technology unit enjoyed, including the supreme sanctions of refusing support for shadow systems or (something like the IT death penalty of the early Internet era) cutting off network connectivity. All of these powers placed central IT at the top or "national" level of the federal pyramid of user relations.

If the first decade of mass Internet usage didn't quite break the federal model of user relations, it put tremendous and distorting stresses on it. At the root of the problem was the geometrically expanding complexity of both enterprise architectures and user demands. Users found new avenues to unmediated expression through technology, first in websites and later through blogs, wikis, and other emerging tools. Self-service via the web made enterprise systems far more visible, changing them from staff-facing systems used during working hours to constituent-facing systems with implied 24 × 7 availability. E-learning introduced major new enterprise applications that served new and increasingly self-aware faculty and student constituencies. Most painfully, the new Internet-based environment brought exotic new forms of malware, enhanced hacking opportunities, and a legal morass surrounding filesharing. Increasingly, the Internet became a vehicle for expressing lifestyles and a battleground for freedom of expression, and the boundary lines between personal, professional, and enterprise concerns became fuzzier still. Demands for support and for computing independence both grew explosively.

IT federalism got more complex but managed to stay functional through all this. At many institutions, the newly conceived role of chief information officer (CIO) put a leadership layer above stovepiped administrative and academic computing divisions. Central IT took on new responsibilities and got new powers, especially in the regulation of security and privacy, which built on its ownership of the network backbone and the major enterprise systems. At the same time, institutions began to formalize IT governance and open it up to a wider range of inputs, recognizing that IT had become a resource relied on by the entire community. Even so, highly autonomous and well-funded local IT units and research labs often found it desirable and feasible to circumvent central IT's systems and policies, while the technology itself—increasingly powerful, inexpensive, portable, networked, and ready to deliver sensitive information—conspired against effective control over the much-enlarged user community. CIOs began to complain that their jobs had become more political and more concerned with risk management than ever and that their practical ability to exercise enterprise authority was diminishing.

## **The Impact of Cloud Computing**

Cloud computing can help address some of the problems that came with the early Internet era. The cloud's democratization of access to computing power is, as we've seen, nothing new; what is new is that cloud resources can at least potentially come with the professional system admin-

istration that personally administered PCs and servers often lack. A user who can fulfill his needs from the cloud will be less tempted to set up the unpatched, insecure, backup-free, under-the-desk rogue server that lies at the center of so many higher education IT tales of woe. Making it easier for users to acquire and maintain the technology they need will reduce certain of the functional/technical demands they place on IT units, and could mitigate at least some of the complexity and exposure that now characterize enterprise IT environments.

But it also seems likely that new complications will attend new simplifications. To a greater degree than ever before, the cloud will make users into choosers who are able to make technology choices without mediation from other parts of the institution. User liberation in the PC and Internet revolutions came with attached strings of dependence that led naturally upward to departmental, school, or central IT units, giving federal relationships some measure of hierarchical coherence. Central IT acted as an intermediary between users and enterprise vendors, which allowed the institution to conduct its relationship with each vendor on a one-to-one basis while extending one-to-many support services to users. This created some valuable symmetries in IT administration: manageability in vendor relationships balanced with scalability in user support and a service provider role balanced with the role of enterprise authority. Users who depended on central IT for connectivity, enterprise agreements, systems administration, and other services knew that their ability to get what they wanted depended (within bounds) on paying attention to what central IT told them to do.

Cloud computing creates new strings of user dependence that lead outward rather than upward, upsetting the balances in institutional and especially central IT authority. Where users directly employ a service from the cloud, they disintermediate institutional IT as a service provider. But that doesn't necessarily mean they eliminate IT as a support provider. Like Wall Street's financiers, users may well be attracted to the chance to privatize reward and socialize risk. There is a danger of cloud relationships that begin as a two-way user-to-vendor interaction turning "triangular" when unhappy cloud users draw IT in for support.

The nightmare scenario for central IT arises when multiple users who have independently drawn collections of cloud providers into institutional business plead *ex post facto* for help to sort out multiparty, multiproduct support issues. Central IT will be tempted to refuse, yet a long history of past efforts to do just that with "unsupported" platforms and applications suggests it will not be an option, at least above a certain threshold. Sooner or later cloud dependencies will create institutional exposures, and the

institution's first reflex will be to turn to IT to address the problem.

This breakdown of symmetry between central IT's ability to shape product choices and its responsibility for user support is only one example of how the cloud can pull mutually reinforcing IT roles apart. Another is the looming disconnect between central IT's service provider role and its responsibilities as enterprise authority. In the early Internet era, CIOs could say to users, "You must use certain precautions and behave in certain ways because if you don't you'll compromise our network and we'll be forced to kick you off." In the cloudy environment, central IT no longer enjoys monopolies on connectivity or access to applications, nor does it have the same ability to define safe harbors and auditable systems. The concerns of enterprise authority—from system and data security to process efficiency and online behavior—will continue to be critically important, perhaps more than ever. Yet they will increasingly be disembodied from the "plumbing" that central IT has historically overseen. Who, then, will speak for the enterprise? And in what tone of voice?

## **Enterprise Authority in a Cloudy Academy**

To some extent, the user community itself will fill the vacuums in support and enterprise authority. Cloud users freed from dependence on the IT bureaucracy may be more conscious of their mutual interests and their ability to self-organize, and the same grassroots self-help impulses that one now sees in open source and Web 2.0 communities could become generalized. Support blogs, wikis, and other collaborative forums will spring up around many cloud resources to supplement vendor support tools. Virtualization and commoditization could also reduce the technical idiosyncrasies users have to grapple with, making it easier for functional user communities to rely on internal support competencies. Nor should we dismiss the possibility that users may develop a more sophisticated and effective sense of enterprise responsibility as they venture into cloud environments. As critics of the idea that every commons ends in tragedy point out, local self-regulation among those most affected by the quality of common resources can be an effective way to protect them.<sup>1</sup>

Yet every shift in computing paradigms has brought its disappointed utopian hopes, and the cloud will be no exception. Computing may, indeed, look simpler to users in a mature cloud environment than it does in today's messy world where desktop, departmental, enterprise, and Internet resources constantly clash; but this, at least, is the devil that institutions know. Besides exposing themselves (and the institution) to the unknown reliability and viability of cloud service providers, users

are bound to discover more subtle limits on the integratability of cloud resources, especially as they begin to mix and match them to support complex processes. These issues will often arise from specific local needs whose unique and possibly confidential nature works against the open source premise that “given enough eyeballs, all bugs are shallow.” More broadly, we need to consider the fact that decades of deploring and fighting institutional stovepiping has resulted in only modest progress toward true enterprise information systems. The centripetal forces that have made enterprise sensibility a constant struggle aren’t going to go away.

How, then, should IT administrators handle a new profusion of outward-leading attachments that bypass the internal controls IT has historically provided? One logical option that will have its adherents is pure *laissez-faire*—neither regulating what users do nor providing institutional support if they get into trouble. But as we’ve already seen, institutional dynamics will likely make this option untenable. Too often in higher education, individual actions lead to institutional sanctions. Institutions can’t simply relinquish due diligence on the grounds of individual choice, and users are certain to run into issues that they can’t address on their own.

## **A Locked-Down Cloud**

On the other end of the spectrum one might envision a locked-down enterprise environment carved out of the cloud. In this model, web traffic entering and leaving the institution would pass through an institutionally managed intermediary that dynamically applies rules about what users can and can’t do. An aggressive implementation might not only block undesired sites in the manner of today’s URL filters but set many terms of use: how long users can remain on a site, what they can download or upload, even what sort of language is allowed when posting to a blog or social networking site. It could also generate a highly detailed record of usage. Institutions would not necessarily have to set every parameter in granular detail; already emerging cloud security vendors such as ZScaler and Purewire promise heuristics-based technologies that assess websites and even personal reputations dynamically.

An environment like this could help institutions contain support demands, reduce assorted kinds of exposure, and keep an eye on process efficiency and staff productivity. Yet it’s hard to imagine successfully implementing this regime in a higher education environment. Even putting aside nontrivial issues relating to user evasion and induced latency, a highly regulated enterprise cloud would be sure to arouse passionate objections on the grounds of academic freedom, personal privacy, organizational unit

autonomy, and incompatibility with modern methods of teaching and research. To put it in the language of civil liberties, a locked-down cloud would constitute “prior restraint,” perhaps justifiable in some settings but completely unacceptable to the sensibilities of an academic community.

## **Certification-Based Cloud Computing**

A much more acceptable way to shape user activity would be to certify rather than dictate good behavior. To borrow a line from pedagogy, central IT might manage a cloudy environment as “the guide by the user’s side,” rather than “the sage on the IT stage.” Web resources could be certified on the basis of good security and enterprise practices, such as use of open standards, robust identity management, encryption and other data management protections, auditability, and business continuity practices. Likewise, certification might address contractual issues such as indemnification, liability, and escrow arrangements in the event of vendor failure or takeover. Users would be encouraged to use certified resources (which would be easily identified as such), warned of the dangers of uncertified ones, and held accountable if they got into trouble straying into uncertified territory.

Certification-based institutional cloud computing would have many of the advantages of a locked-down cloud, such as rationalizing support needs and articulating enterprise requirements, but would be more open and politically sustainable and would better leverage the advantages of the cloud. Presumably, certification would be a collaborative process involving multiple concentric rings of participation. At the core, a basic set of enterprise certification guidelines could specify institution-wide practices, drawing on input from surrounding rings of school, departmental, and user-group entities and deferring to them on matters of local scope. Surrounding these would be additional rings representing external communities of practice, standards bodies, product user groups, and other entities with relevant expertise.

While it’s likely to be a better fit both with the spirit of cloud computing and with the culture of higher education, a certification approach has its problems. It obviously places a great deal of hope on the slender reed of standards and certification assessments. Standards processes are notoriously slow and prone to the disproportionate influence of interested parties; they are subject to interpretation; and they can be either too general to be meaningful or so detailed as to be impossible to implement. Even when standards are clear and up to date, deciding whether a particular resource meets a given standard requires investigation and judgment. Nor is it entirely clear what kinds of standards cloud computing

might call for. Moving toward a trustworthy cloud computing resource “seal of approval” requires a leap of faith that global and local computing communities can create all the necessary processes.

Even if that faith proves well founded, a certification approach to cloud computing will require some potentially disruptive changes in relations between IT units and users. The most obvious one is deciding who does the certifying and through what process. Users who have discovered a cloud resource that seems to meet their needs perfectly may well resent a third party’s refusal to certify it. At the innermost level of certification guidelines, central IT is probably the best candidate for overseeing the process, in part because it is the entity with the best ability to provide support to users of certified resources, and in part because of its enterprise experience. Both the realities of higher education culture and the logic of the cloud, however, would demand that certification be an open and inclusive process. In parallel with the certification process, both central and local IT units could also help users assess vendor certification claims and sort out the institutional implications of what might be a confusing tangle of competing standards. Influence of this kind could enormously reduce institutional exposure and improve the cloud computing experience for all users.

A second issue raised by a certification approach is how to enforce user accountability. Even in a fairly open “use what you want but be accountable” environment, enterprise considerations will demand some degree of user monitoring (such as usage logs and audit trails), particularly because in a cloudy environment fewer resources have the implicit controls that come with institutional ownership and physical control. Who will be in charge of monitoring the trails users leave in this environment, and who will deliver sanctions when they step out of bounds? Central IT can best influence accountability indirectly, for example, by building appropriate auditability into its resource certification processes. But enforcement responsibility and the setting of sanctions in this exceedingly sensitive area ought to lie with the authorities users are most likely to consider legitimate: themselves, their managers, and the executive hierarchies they fall under.

## **IT’s Changing Responsibilities**

It seems clear that the cloud’s transformation of users into choosers will cause some power to flow “downward” in the IT federal hierarchy. Probably the greatest beneficiaries will be at the middle levels of the hierarchy, among business and academic units that gain not only IT independence but perhaps also budget dollars that are reallocated when

central IT-delivered services become, in effect, business services contracted from cloud providers. Researchers, already the most independent of institutional users, will have still more opportunities to break from institutional constraints. Individual staff and student users might see radical or limited changes, depending on their needs and their willingness to venture beyond the realm of certified, supported computing.

Yet as some of the IT organization's responsibilities fade, others will remain and new ones will emerge that have no obvious "owner" other than a central IT unit. "Chooser" support is one of these, and it implies a more or less formal process of cloud resource certification that can become a potent, though indirect, protection for the enterprise. That in turn leads to perhaps the most important central IT role that will carry over into the cloud era: definition and management of institutional IT governance. The cloud's liberation of unit-level and individual users is an inherently politicizing trend that will feed demands on governance, because it means that enterprise policies once implicitly embedded in institutional service delivery will have to be negotiated (or mandated) explicitly. No one has the experience that central IT does in dealing with such enterprise IT politics. As a recent ECAR study of IT governance found, responsibility for IT governance is overwhelmingly in the hands of CIOs, and they tend to run inclusive and, by their assessment, effective governance structures.<sup>2</sup> IT leaders who wearily describe their role as "herding cats" may well be identifying just the sort of experience and skill that will keep central IT strategic in the age of the cloud. Likewise, today's focus on risk management and legal issues is a likely harbinger of the central IT skill set of the cloud era.

As the example of IT governance suggests, declining IT unit control over hard resources will make the ability to exercise "soft power" more and more central to the unit's existence. Additional responsibilities in this vein may include monitoring cloud resource usage across the institution, assessing the efficiency of processes that cross departmental domains, contributing to institutional information architecture and strategy, and architecting the local infrastructure (especially identity management) to permit seamless and secure access to the cloud. The common thread in these tasks will be the need to meet enterprise responsibilities through influence, negotiation, and informed risk management rather than through official enterprise authority.

## **Conclusion**

There are, of course, many considerations that could prevent the full logic of the cloud from being realized. The cloud has not yet proved its

ability to deliver cheap, scalable, virtualized computing power; still less its potential for loosely coupled integration; and least of all its radical promise of modular applications built from mix-and-match services. The decisive failure of cloud services could reinvigorate “classic” centralized enterprise computing, and even if the cloud is successful, the transition from locally hosted to cloud resources is likely to be gradual and bumpy. But in proportion to the degree that the cloud achieves its promises, it will shift power downward in the IT hierarchy, atomize enterprise IT authority, and reshape central IT’s role from service provider to certifier, consultant, and arbitrator. Central IT will need to better master the arts of soft power to continue to play its vital role of articulating and protecting enterprise interests.

## Endnotes

1. Garret Hardin, “The Tragedy of the Commons,” *Science* 162 (1968); Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge and New York: Cambridge University Press, 1990).
2. Ronald Yanosky with Jack McCredie, *Process and Politics: IT Governance in Higher Education* (Research Study, Vol. 5) (Boulder, CO: EDUCAUSE Center for Applied Research, 2008), <http://connect.educause.edu/Library/ECAR/ProcessandPoliticsITGover/47101>.

## Bibliography

- Hardin, Garret. “The Tragedy of the Commons.” *Science* 162 (1968): 1243–48.
- Ostrom, Elinor. *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge and New York: Cambridge University Press, 1990.
- Yanosky, Ronald, with Jack McCredie. *Process and Politics: IT Governance in Higher Education* (Research Study, Vol. 5). Boulder, CO: EDUCAUSE Center for Applied Research, 2008. <http://connect.educause.edu/Library/ECAR/ProcessandPoliticsITGover/47101>.