virginia.edu
The Information Technology Magazine at the University of Virginia

IT Policy: From Policy to Polity, and Back Again

by Chip German
Director, Policy and Planning
Office of Information Technologies
University of Virginia

[*NOTE: Original graphics not available with this version*]

Perhaps a brief introduction is in order: I am the person responsible for policy development in the University of Virginia's Office of Information Technologies. As exciting as that responsibility sounds, I have to admit to bringing an unusual perspective to it. I am hostile to the notion of developing policy when you don't need it, and I carry a prejudice against policy that is written as though there is something unique about the "digital" environment.

Sure, sometimes computer-usage policies are unique to their context, but mostly they find the best effect when they simply help the folks who use computers realize that the rules of the rest of society can and should be applied to the world of bits and bytes.

The "Vertical Accretion" Model

Which brings me to the subject of this column. I write today about one way to approach constructing policy for the digital environment. The approach is particularly appropriate to an academic community and entirely unoriginal, although I will happily take full credit for it. From time to time accompanying my description, you will find illustrations intended to graphically represent important profundities. The first profundity: Figure A depicts how we often develop computer usage policies. I call it "Policy Development by Vertical Accretion" with the subtitle "Stalagmites in the Computing Cave."

In this approach to policy construction, things start with an event—an offense by a computing malfeasor (technical translation: some poor sap acted like a three-year-old and got caught at it). The horrified authority hierarchy (this includes me), fearing either (a) the likelihood that repetition of the act by others represents a real threat to the fabric of the University community or (b) the repercussions on state funding if legislators learn such a thing can happen at the University, concludes it must act decisively. A specifically worded policy emerges that clearly declares the behavior involved verboten.

Unfortunately, computing malfeasors are experts at exploring the edge of the policy envelope, so the next event is usually just enough different technically from the first that the miscreant mounts a defense claiming the specific language of the policy doesn't cover his action. A legalistic debate ensues in the setting of whatever disciplinary process can be brought to bear on the question: technical experts are brought in to explain, variously, why the policy does or does not apply. A collection of the malfeasor's peers judges the matter, and in subsequent iterations, the policy is refined and

redefined by "case law" into a concept that must be interpreted by lawyers, psychics, and other highly compensated consultants.

Hyperbole, you say. But the point is important. Policy built from individual events tends to be rigid, limited in scope, and difficult to apply. Although few systems of policy are completely based on individual events, many have fundamental components that came from such sources. I also believe that this kind of policy development is characteristic of "emerging" environments—as networked computing has become a general utility rather than a service designed for and used solely by scientific specialists, we've rapidly had to develop policies for the general population. In the absence of a longer historical perspective on the digital world, most of us have patched together an overview to guide policy by finding the common elements of how we handled a collection of individual events. But now the usage environment is maturing, and we've had time to understand better the relationship between policy and the reasons we create it. What is emerging is a new capacity—we now can begin to see the outlines of the kind of digital community in which we want to live.

The "Community Vision" Model

Hence the notion of "Policy Development by Community Vision," subtitled "Common Sense and Horizontal Integration" (Figure B). In this model, a community that has begun to understand the range of behaviors that occur in a digital environment determines how it wants itself perpetuated in that environment. Here at the University of Virginia, we refer to ourselves as the "University community," with a pretty good idea that the notion of community extends to faculty, staff, and students, and often to families and to library patrons, and sometimes to neighbors and visitors as well. It is not simply a regulatory concept; it is a social one too. We teach, study, work, and live in this community context, but we also pursue entertainment and recreation, some are born and die here, and we conduct the financial aspects of our lives in it. This community is bound together by a common appreciation for the life of the mind, but that life is quite broadly defined and doesn't reside solely within classrooms, workspaces, or dormitory rooms.

Logic would suggest that the University community will not be able to define how it should be manifested in the digital environment any better than it can define itself in general, but the work several years ago to define the University vision known as the Plan for the Year 2000 provides a good sense of desirable community elements. Such notions as open exchanges of ideas, safety and security for those pursuing the life of the mind, and the importance of intellectual activity not being bound by physical or organizational barriers pervade the document. Another important notion deeply woven into the fabric of this place is that of honor—that members of the University community are willing to stand and be accountable for their actions. Such concepts can be quite helpful in defining principles of policy for the digital environment.

Questions that Must Be Answered

Doing so in this way is an inversion of the previous model: you don't build policy up from events, you build it down from vision. The trick is articulating a vision on which the community can agree. That's the stage we're at now. Our organization is working with the University Committee on Information Technology to see if we can draft a vision of how the notion of University community applies to our digital environment. Already I can imagine some of the questions such a vision should answer:

- What do we mean by the term "privacy" for members of the University digital community?
- Do we want to ban commerce from our digital community or do we want to define the place and manner in which it can exist?

- How do we want to balance the notion of free exchange of information with the need to respect the intellectual property of others?
- How do we want to balance the notion of free expression (and its occasional companion on the Net—profane or abusive speech) with the desirable atmosphere of civil discourse in an academic community? Is this another place-and-manner question?

From the answer to such questions comes guidance for policy creation. Take the privacy question as an example. We know that the University as an employer can legally have access to employee electronic mail files. But we also know that the University can install video surveillance cameras to monitor employee work areas—it has chosen not to except in limited, specific circumstances and has established policy to this effect. Under the old "accretion" model of policy development, that decision exists in relative isolation. But using the community vision technique, we can consider more effectively what the video-camera policy says about the kind of community we are trying to create and apply the lesson to defining privacy in the digital community. In this model, we can ensure that policy is more readily "horizontally integrated," forming a consistent system that is easier to apply, in part because it comes from a common community understanding.

A Statement of Vision

So it isn't hard to imagine the product—a vision of digital community. It should be relatively short—a couple of pages—and to the point. It might start like this:

The University community is a diverse collection of persons joined by a common purpose—the pursuits of a life of the mind, consistent with the mission of the University of Virginia. When that community, or parts of it, convene and converse with the aid of the digital medium of electronic communications, the community has expectations about the nature of the discourse that takes place in that medium similar to those about the nature of community discourse in other forums and forms.

To that end, the community observes the following principles of university life in the digital environment:

- Access to the digital environment often has real costs, so the University is unable to offer full access to all interested persons. At the same time, accountability for behavior in the University's digital environment is related to a person's affiliation with the University. If someone has no stake in holding and keeping an affiliation with and access to the University, then that person has no built-in incentive for conduct that contributes to it as a community. For those reasons, the University limits participation in many aspects of its digital community to persons with formal affiliations to it.
- Accountability in the University community also involves the same principles on which the University's Honor System is based—that persons will come forward and be accountable for their actions in a community of trust. As a result, hiding one's identity to avoid accountability in the digital community is a serious transgression.
- Privacy in the digital community means that members of that community have a reasonable expectation that their personal electronic files and communications will remain private, unless they are informed in advance that privacy will not be protected in specific circumstances and settings. However, this principle is not absolute—the privacy of individual files or communications can be overridden by the actions of a court of law, by similar process of disciplinary bodies within the University community, and even inadvertently by technical staff who are operating in good faith to resolve technical problems. The community expects

that privacy will be protected as much as is practically possible given these conditions, except in specific cases in which the affected community members are informed in advance.

- In a community based in large part on intellectual activity, one of the most broadly supported and easily understood principles is that of the protection of intellectual property. It is the responsibility of all members of the University's digital community to become familiar with and observe guidelines on the protection of intellectual property, no matter who is its owner.

That is the Mom-and-apple-pie stuff. We'll encounter much more complexity as we try to sort out issues involving content of communications and some of the other questions I described earlier. As I mentioned, this process is under way now.

virginia.edu, Volume I, Number 1, Spring 1997

Published by the Office of Information Technologies (OIT) and the Department of Information Technology and Communication (ITC) at the University of Virginia