UA Regulation Critique

Abstract

The system collectively called the UA Network is an extremely large and complex system. It takes in at least four major networks (UA Statewide, UAF, UAA, and UAS), several smaller networks (e.g. ARSC, GI, and UAF extension campuses), houses major databases (e.g. Banner), and probably hundreds of department level databases, is connected to thousands of computers, and directly or indirectly affects tens of thousands of people, not just users. So it stands to reason that the integrity (both data flow and data itself) of UA Information Resources must be preserved. The Regents Regulation R02.07 attempts to lay down rules that will serve to this end.

The Regulations are well thought out, and it is evident they were assembled by a group knowledgeable in Information Technology. They clearly spell out what a users and administrators may not do, and what will happen when these rules are breached.

An underlying theme through the regulations is that of academic freedom. Opinions may not be censored, and privacy must be protected. These are noble goals, and I appreciate their stance. I am concerned, however, that these ideals may face some tough challenges in the coming months or years. They may required to search through “private files” for “suspicious” information. It will be interesting to see how this plays out in the future.

Authorship and Detail

One of the things that comes through when reading the policy and regulations is they were not made exclusively in a political environment devoid of technical know-how. The operational procedures mentioned and the terms used show an understanding of information technology, and the some of the special considerations that are necessary to regulate it.

Arguably, the most important part of a set of regulations is the set of terms that will be used, and their associated definitions. Government usually does a great job of defining words and phrases, and the UA Regulation is no exception. Terms are clearly defined, and their scope (the context in which they apply) is spelled out.

As with most documents that try to regulate a rather ethereal medium, one in which there are so many things one can do, there is very little regulation as to what one *can* do. It mostly talks about what one *cannot* do. To draw an analogy to access control, the order is deny, allow; deny from all, allow some: You are allowed to do it, unless they say you aren't.

Policy to Regulation

The UA Regents' Policy sets out the general guidelines for, in this case, Information Resources (IR). From the perspective of policy, the policy is complete as it should be. It defines what it is talking about, who a user is, the objectives of managing information resources, and basic access, conduct, and enforcement guidelines, all of which are expounded upon in the regulations.

Definitions

The UA Regulations says that "Information Resources include information systems and information networks owned, leased, or operated by the University, as well as the information (e.g., text, data, or software) resident on systems or carried over networks. This definition applies to all Information Resources acquired and controlled by:" system administration, i.e. UA Statewide, university campuses, departments or other units, individual faculty, staff, and students, in their capacity as University employees. "This definition does not depend on the source of funding for Information Resources. Information Resources acquired through grants, contracts, or donations are included." So, if it is data, transmits data, or stores data, it is an "Information Resource." This definition is broad enough to cover telephones and fax machines, as is seen the definition of a network (below). This could arguably be used to give the "computer guys" much broader jurisdiction than they currently enjoy. In fact, there is some

rumbling—the final outcome remains to be seen—that telephone services may be moved under DC&C.

As user is defined as “an individual who accesses, transmits, or stores information on an information resource. Users include (but are not limited to) students, faculty, staff, and affiliates of the University given access to University Information Resources. Users also include guests and visitors of the University, as well as members of the public who access, transmit, or store information on an information resource.” This is where the Regulation shows a bit of its bureaucratic bloat. It seems like it could have been as simple as saying a user is anyone who uses the facilities of an IR.

A System Administrator is one who manages an Information Resource (e.g. server, network component, database) in his day-to-day function. They have special consideration, and special rules, because they have “extraordinary access” to the information contained on, and passing through, these systems.

The network “designates the physical infrastructure that carries voice, video and/or data within an MAU up to and including connections to external networks or providers.” This includes all the hardware and software used in the network, “up to but not including end-User devices such as desktop computers, printers, or telephone handsets.” This definition is evidence of either a) the broad scope of what IR is considered to be, or b) evidence of micro-management. If telephone refers to a standard telephone, then analog voice systems are included in the definition of IR, and fall under these regulations. If it refers instead to an IP telephone, then someone was thinking at a level way too detailed for that statement.

There are other terms defined in the regulation, but they are not germane to our analysis.

Clarity in Purpose

The objectives in the UA regulations spell out the purpose very clearly. While wanting to promote academic freedom, I’m sure, they seem to serve to mostly protect the university of liability and breech of confidentiality. I find it somewhat amusing that the first objective is “Respect First Amendment rights and privacy of persons,” and last objective is “Minimize legal liability of the University related to Information Resources.” The section on administrators, to be discussed below, is very specific about what system administrators can and cannot do. Included in the list of things an administrator cannot do is browse files in user directories (unless required in a maintenance capacity) or gather information that would reveal usage patters, unless authorized as part of an investigation. However, depending on the way the laws go in the next few months, administrators may be required to do both these things on a regular basis, even if there is no ongoing

investigation. Scanning for "suspicious files," such as files containing blacklisted keywords, or encrypted files, or watching for suspicious actions, may be required soon. In addition, "reducing liability" may proceed to the point where offending material must not simply be removed upon discovery, but actually must be scanned for proactively. It will be interesting to see how this is played out in light of the current University Regulations.

Conducting One's Self

The "Standards for User Conduct" list the overall expectations of a user, and are quite reasonable, not making any demands that would be difficult for a user to follow. The first thing it does is to remind users that there may be other factors weighing in on the legality of actions. More than just R02.07 govern usage of computers in the UA system: rules laid down by other UA regulations, or by law, may determine what a user can or cannot do. It then goes on to say: don't use UA IR to harass; obey copyright laws; don't modify data without authorization, and don't do anything that would damage the system; no anonymous e-mail or other communication; must obtain access through established channels; don't crack passwords; don't use an inordinate amount of resources; realize that security isn't perfect and files may be viewed by unintended parties, especially law enforcement, should an investigation require it; make it possible for authorities to access protected or encrypted data. Some of these are just restatements of state or federal laws already in effect, and it seems they could easily have been left out. Or, more appropriately, placed in a procedures/orientation manual where it might be more likely to be read.

Freedom of Speech vs. Administrative Oversight

It is the desire of the University to not limit "free speech" or academic freedom. Thus, the regulations are careful to have very specific, and legitimate, reasons for restricting the content that may be stored and transmitted in the UA IR.

Discussion forums may be limited to topics at hand, but cannot be moderated based simply on viewpoint. However, there are some potentially interesting tests of this clause. A user may claim the discussion they started does fit in the topic of the group when the moderated says otherwise. Example: a forum for discussing reducing the teen STD rate. For most people, this means talking about condoms, safe sex, etc. But some may try to discuss abstinence as a method to achieve the desired end. The majority may claim it is off topic; the minority may claim their viewpoint is being censored.

Large mass mailings, as well as other activities that consume large amounts of resources, may be restricted so the resources available to other uses will not be reduced to unusable levels. There cannot be explicit (or apparent) endorsement

of commercial entities. The University desires to appear impartial, and thus cannot promote any specific company. And finally, any material that is simply illegal, for example, obscene material or efforts to incite violence, are also prohibited.

Bad User! No Network!

If these regulations are violated, there are procedures of discipline. The steps allowed are fair and reasonable, especially considering the kind of damage a breech of security may cause. An employee may be terminated, and a student expelled, for "violations of the standards" of conduct. For "lesser crimes," access to IR may temporarily restricted or denied. If their action has violated law, they may also be subject to criminal prosecution.

Protecting Privacy

Section R02.07.060.C of the regulations lays down some very specific guidelines when it comes to user privacy, and what administrators can do in regards to user files. The justification for this protection of privacy is, of course, academic freedom. Only in the "line of duty" may IR personnel "access the content of electronic communications and copy and examine any files or other information resident on or processed through Information Resources." Users are given "a reasonable expectation privacy."

R02.07.060.C.2 says that IR personnel "shall maintain confidentiality of files and information (other than evidence of conduct threatening the security of Information Resources)." This information may be disclosed, following proper procedure, to law enforcement, if there is evidence that a crime is taking place, or is about to.

One clause in this section is bit puzzling. It says that files may be voluntarily disclosed to law enforcement, if it is judged that the files are in violation of state or federal law. It does not mention how these files would be discovered (i.e. no "in line of duty" clause, as in other cases), so it leaves one to wonder if this loophole is left open for spot checks.

Into the Fog

One of things that is a bit disconcerting about these regulations is that the majority of the sections were last updated in January of 2001. While these regulations still apply quite well, information technology has changed quite a bit since then, and it would behoove the regents to see if sections may be reworded or defined more closely.

One of the major problems seen with these regulations are their ability to be extremely vague. There is no definition of the types of network activity that are prohibited. An (in)famous example is that of port scans and ping sweeps. Port scans will get you a warning with DC&C, but this activity is not mentioned, nor is it mentioned in the latest UAF policy FAQ.

In addition, section R02.07.052.D says activities that use "Disproportionate or Debilitating Amount[s] of Resources are not allowed. But, it does not then define what is "Disproportionate or Debilitating." On-campus transfer can easily average two Mb/s, with spikes up to four or five. But is that using too much? How long before you're using too much resources?

In Conclusion…

The regulations for Information Technology for the University seem to be well put together, overall. There do seem to be holes and inconsistencies that may be good to review and close to make them more consistent and less vague.