Fall 2005

# ACUTA Journal of Telecommunications in Higher Education

# acuta Journal

## of Communications Technology in Higher Education

Washington,DC Convention & Tourism Corp.,Jake McGuire.com

This Issue: Legislative and Regulatory Issues

# Events Calendar

| Event | Date | Place |
|---|---|---|
| **Fall Seminars** | October 30 – November 2, 2005 | Marriott City Center<br>Denver, Colorado |
| **Winter Seminars** | January 8 – 11, 2006 | Renaissance Esmeralda Resort<br>Palm Springs, California |
| **Spring Seminars** | April 2 – 5, 2006 | The Westin Providence<br>Providence, Rhode Island |
| **Annual Conference** | July 23 – 27, 2006 | Renaissance Esmeralda Resort<br>Palm Springs, California |

**ACUTA's Core Purpose is to:** Support higher education communications technology professionals in contributing to the achievement of the strategic mission of their institutions.

**ACUTA's Core Values are to:**

- Share information, resources and insight,
- Respect the expression of individual opinions and solutions,
- Maintain our commitment to professional development and growth,
- Advance the unique values and needs of higher education communications technologies, and
- Encourage volunteerism and individual contribution of members in support of organizational goals.

**acuta**

# Contents

**"**VoIP threatens to undermine virtually every aspect of traditional telecommunications policy, and for that reason, it is likely to trigger a much-needed regulatory revolution."

Jeff Linder, Wiley Rein and Fielding
*page 10*

# The ACUTA Journal of Communications Technology in Higher Education

**Submissions Policy**

*The ACUTA Journal* welcomes submissions of editorial material. We reserve the right to reject submissions or to edit for grammar, length, and clarity. Send all materials or letter of inquiry to Pat Scott, Editor-in-chief. Author's guidelines are available upon request or online at www.acuta.org.

The opinions expressed in this publication are those of the writers and are not necessarily the opinions of their institution or company. ACUTA, as an association, does not express an opinion or endorse products or services.

*The ACUTA Journal* is published four times per year by ACUTA, a nonprofit association for institutions of higher education, represented by telecommunications managers and staff.

Visit the ACUTA site on the World Wide Web:
**http://www.acuta.org**

**Membership and Subscriptions**

Subscriptions are provided as a benefit of membership. The publication is available to nonmembers for $80 per year or $20 per issue. For information, contact Kellie Bowman, Membership Development Manager, 859/278-3338, ext. 22, or e-mail, kbowman@acuta.org.

# With a Fluke Networks' portable analyzer, expect to be seeing more of these.

Sorry I said it was the *network's* fault
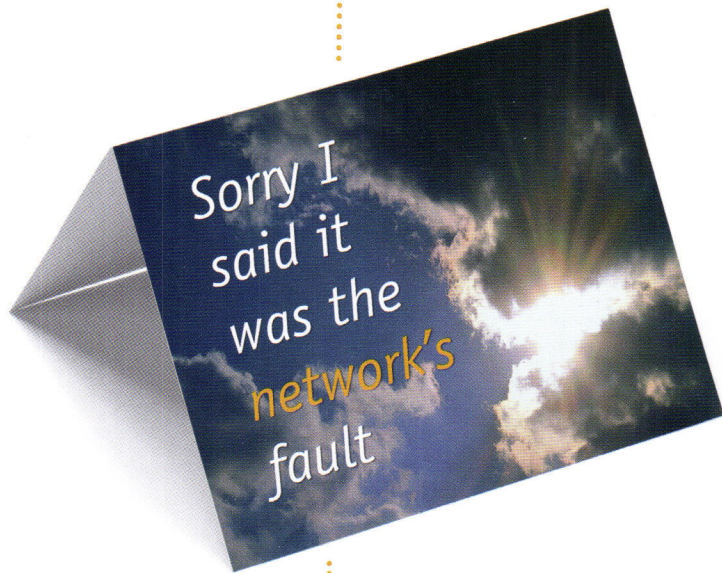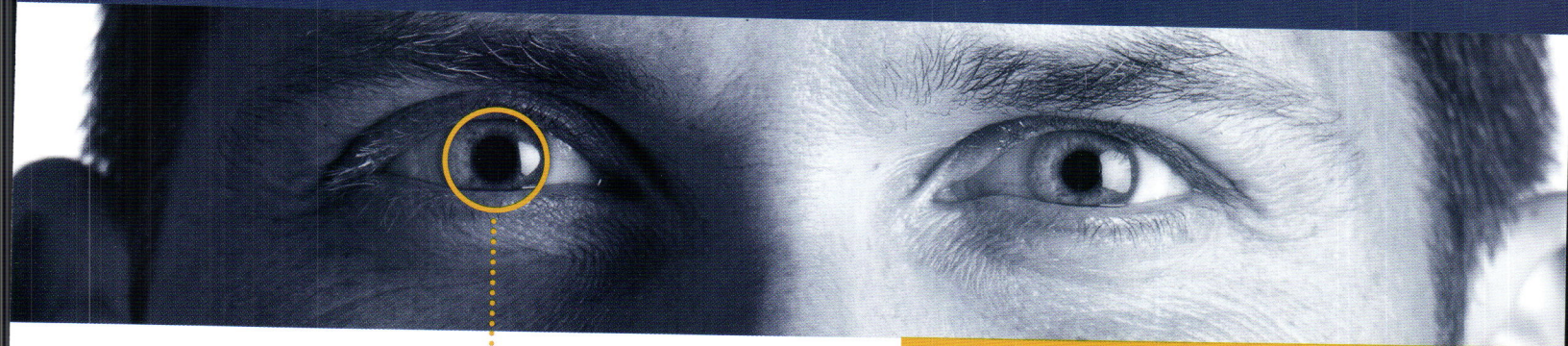
**EtherScope and OptiView – Two Portable Network Analyzers created to help prove it's not a network problem. Faster.** Quickly proving problems are not network problems is exactly what our portable analyzers are all about. Unlike a protocol analyzer or laptop freeware, they give you the complete vision you need to quickly and accurately diagnose problems. For example, you can track down connectivity problems and incorrectly config-ured stations, identify causes of network slowdowns (like excessive broadcasts) and spot bandwidth hungry applications. All with one tool: a Fluke Networks' portable analyzer. Simply put, they're the best way to prove it's not the network's fault. And the surest way to start getting a little more respect around the office.

**Prove it's not the network's fault. Faster. Visit www.flukenetworks.com/PNA to see how one of our portable analyzers can make your job easier.**

**NETWORKSUPERVISION**™

**FLUKE**
*networks*

## PRESIDENT'S MESSAGE

Patricia A. Todus
Northwestern University
ACUTA President
2005–2006

# Regulatory and Compliance Issues at Northwestern

Northwestern University focuses on federal and state regulations and compliance issues on several different fronts. As an R1 research university with a medical school, we must adhere to numerous regulatory and compliance requirements in addition to those facing non-research educational institutions. To that end, a number of internal offices and committees work together to address these requirements.

The office of research integrity within the office of research has been established to help our research community better navigate the myriad of expectations and responsibilities that come from conducting research. One of the responsibilities of this office is to monitor our research activities from a regulatory perspective and educate our researchers about regulatory and compliance requirements.

A director of information and systems security/compliance was recently added to the information technology staff. His department's responsibilities are to provide leadership and guidance to the Northwestern University community in the areas of information security and compliance issues. This includes raising awareness by educational initiatives, development of policies and standards, and the monitoring of government regulations and compliance requirements. A security/compliance program has been established, and a committee of University representatives is in place to provide ongoing policy guidance and determination of which elements of the program should be addressed each year through risk evaluations and their understanding of the changes, present or planned, throughout the University.

The auditing department of the University also has taken an active role in regulatory and compliance issues, in their independent capacity of evaluating risk, control, and governance processes. Auditing has formed a compliance committee that includes representatives who have compliance responsibility for all of the major departments of the University. The committee acts as an oversight group and provides a venue for information-sharing and raising awareness.

A recent addition to the auditing department staff is the director of compliance. This director, while not responsible for compliance throughout the University, is the administrative overseer of the University ethics website and hotline. The website and hotline provide information on ethics policies and compliance with regulations, and the accompanying telephone hotline allows University staff, faculty, and students to raise concerns anonymously about potentially unethical behavior or inappropriate actions by members of the University community. The director of compliance ensures that these concerns are investigated appropriately and in a timely manner. In addition, the director is also responsible for risk assessment, assessing compliance gaps in schools and departments.

The regulatory and compliance issues in an institution of higher education have substantially increased over the years. Some believe these recent increases are a result of events on September 11, 2001. While this tragic event had a major impact on the number and kinds of regulations and compliance issues we now face, the very complexity of our institutions has

predisposed us to a variety of regulatory and compliance standards. For example, long before September 11, protecting the rights and privacy of our students produced critical regulatory and compliance issues for higher-education institutions.

There is no doubt that the increased complexity of the world we live in today, combined with the many complex facets of a higher-education institution, has required more knowledgeable staff, policies, plans, and procedures. This is a time of change and a challenge for those of us in information technology. It is also a responsibility. We must ensure that our campuses are adhering to regulatory and compliance issues through campus collaborative activities and the addition of staff experts. It is also important that we take a proactive role and influence the development and review of regulations and compliance requirements.

With the appointment of Tamara Closs to the FCC CAC (see page 15), ACUTA is now represented at the federal level as our government representatives review information technology issues that affect the ways we communicate globally from our institutions of higher education.

ACUTA truly stands out as a professional organization that not only has member experts in this arena, but provides all of us with ongoing information about regulatory and compliance issues and policies.

As you read this issue of the Journal, you will be impressed with the knowledge of your peers and see, once again, how valuable the network is that allows us to share our experience and our expertise, in this case, in the legislative and regulatory arena .
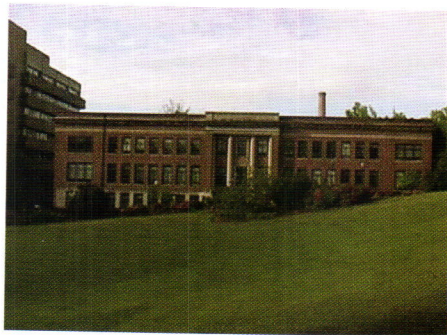
▼

# Reflecting on an Eventful Year

Jeri A. Semer, CAE
ACUTA Executive
Director

I recently had the pleasure of reporting to the Annual Business Meeting on the activities of the past year. For those who were not able to be at the outstanding 2005 Annual Conference (rated best for presentations of any conference in recent memory, and with the largest exhibit hall ACUTA has had in years!), I'd like to cover just a few highlights of the 2004-05 administrative year.

It is a pleasure to be able to work with the creative and energetic professional staff in the Lexington office, who continued to provide outstanding service to our members. I believe that the continuity of the staff team continues to benefit the ACUTA organization.

We also enjoyed the leadership of a very talented and hard-working group of elected and volunteer leaders—our Board of Directors, committee chairs and committee members—who continue to devote tremendous energy to setting a wise course and keeping ACUTA moving in the right direction.

## Strategic Planning

The professional staff was very pleased to have had the opportunity to be involved in the strategic planning process, working with all of the committees and the Board of Directors to examine ACUTA's mission and goals.

The staff also contributed our thoughts and suggestions on the implementation phase, working closely with our committees as they developed recommendations for specific action items and target dates to translate the mission, goals and objectives into operational plans for the next three years. Many of the action items cross committee and departmental lines, and the staff will play an important coordinating role.

We have already begun working on several of the action items in advance of their targeted completion dates, such as the communities of interest, the white paper series on public policy and other issues, participating in issue-based coalitions, seeking appointments to key FCC committees, increasing our media visibility, and others. The staff is energized and committed to helping ACUTA achieve its mission, and we appreciate being included in the process.

## Public Policy and Regulatory Affairs

As the staff liaison to the Legislative/Regulatory Affairs Committee, I spend a great deal of time monitoring developments at the U.S. Federal level and key state developments. It has been a fairly active and fast-paced year.

We completed a study of the potential impact of various proposed universal service funding mechanisms on our member institutions. We also recognize the importance of working closely with the higher education community on public policy issues, and I participated actively with other associations on coalitions on such issues as the Communications Assistance for Law Enforcement Act (CALEA), universal service, re-write of the telecommunications laws, and community broadband networks. ACUTA is recognized as an important and respected contributor to these coalitions.

I believe that ACUTA has benefited substantially from the increased involvement of legal counsel on regulatory and legislative issues, made possible by the commitment of our Board of Directors and membership support for making this important investment.

With their support and assistance, our online Regulatory Issues Matrix has grown into a very valuable document updated quarterly, which I hope you are using to advise your campus on the important issues we are currently following at the Federal level.

We also published twelve issues of the Legislative/Regulatory Update, our online newsletter which is a joint effort with Wiley,

Rein and Fielding, in addition to submitting comments to the FCC and FTC on five different proceedings, issuing several alerts to ACUTA members, and keeping the resources on the legislative/regulatory pages of the ACUTA website up-to-date.

### Public and Media Relations

We have begun a concerted effort to increase ACUTA's proactive involvement in media relations. The main goal of this public relations program is to position ACUTA as a valuable source of information about technology in higher education, consistent with our strategic plan. We want to make ACUTA better known among editors, so they turn to ACUTA and its members as sources for comment on issues and input for articles.

ACUTA is receiving an increasing number of requests for comment from the media, including higher education and technology publications and even the mainstream public press. For example, we received a request for comment from the Washington Post on student use of cellular phones, and ACUTA was quoted on the front page of the Post earlier this year.

This media interest contributes not only to the visibility of ACUTA as an organization but, equally important, to the visibility of our members and the importance of communications technology on your campuses. Whenever possible, we refer reporters who call us to ACUTA members, who can discuss the requested topics with expertise and campus experience.

At the Annual Conference, we conducted a training session for members to serve as spokespersons for ACUTA with the press. We have also increased the frequency and number of press releases we send, and expanded our media list for distribution of press releases. We are also actively pursuing opportunities to place articles about ACUTA and communications technology in various publications. These are just the highlights of our media

relations effort, and it is already resulting in increased visibility.

### Association Operations

Some of the other new areas that we focused on this year, in addition to ongoing programs, were:

• We conducted two regional workshops, designed to bring ACUTA quality education to the local level for members who may not have the time or budget to travel to our national events.

• We completed a major upgrade to the software we use to manage ACUTA's membership database, which will result in increased capacity to meet member needs by helping us better understand the history and professional interests of our members, and improve the accessibility of member records and services through the Web.

• A multi-disciplinary staff team developed a disaster recovery and

business continuity plan for the ACUTA headquarters operation.

• We conducted numerous surveys and market research projects in support of association programs and services.

• We supported the development of the Communities of Interest pilot project, and will work actively with the VoIP Community of Interest steering committee to make this new program a valuable service for ACUTA members.

None of these actions could have been accomplished without the dedication and energy of every member of the ACUTA staff and volunteer leadership team. I would like to thank everyone for their professionalism and commitment to the continued success of ACUTA.

*Reach Jeri Semer at 859/278-3338 or jsemer@acuta.org.*

# The Coming Voice-over-IP Revolution

Jeff Linder

Wiley Rein & Fielding

Things in Washington, D.C., don't usually move quickly, which is probably for the good. After all, "first do no harm" is sound advice whether you're a doctor or a policy maker. Political disagreements and the competing interests of different industry segments usually ensure that change is incremental and that laws and regulations don't swing too far in any particular direction.

There is a downside to gradualism, however. When changes build up incrementally over time, the overall policy picture can become muddled and inconsistent. That is certainly true in telecommunications today, where competing service providers are treated differently simply because they use different technologies or originally came from different market segments.

Rationalizing telecommunications regulation should be a top priority. The telecommunications industry drives economic development, and the deployment of broadband technology engenders unquestioned social benefits, including distance education, telemedicine, and telecommuting (not to mention access to online music, movies, and games). But if policy makers are slow to act (or, more accurately, to react), the confused policy environment likely will delay and diminish investment in broadband.

To his credit, the new chair of the Federal Communications Commission (FCC), Kevin Martin, has stated that fostering a deregulatory, pro-investment environment for broadband will be the principle focus of his leadership. That policy goal is laudable. Achieving it, however, will be difficult, because reforming regulation is likely to mean a change in the roles of federal and state regulators and a shift of billions of dollars among different portions of the industry.

Luckily, there is a powerful catalyst for change: Internet protocol (IP)–enabled services and, in particular, voice over IP (VoIP). VoIP threatens to undermine virtually every aspect of traditional telecommunications policy, and for that reason, it is likely to trigger a much-needed regulatory revolution.

Against this background, this article will consider the potential impact of VoIP on three pillars of traditional telecom regulation: the division of regulatory authority between the FCC and the states, the rules governing inter-carrier compensation, and the system that supports universal service.

## An End to State Regulation?

For more than 70 years—since passage of the 1934 Communications Act—the FCC and state regulators have shared jurisdiction over telecommunications services. Interstate services are subject to the FCC's authority, and intrastate services are subject to state jurisdiction.

At first, both the FCC and its state counterparts regulated the rates charged by service providers and the entry of new competitors into the market. With the rise of long-distance competition in the 1970s and 1980s, federal and state regulators relaxed rate regulation and market entry requirements for interexchange carriers. Similarly, following the advent of local competition in the mid-1990s, states reduced regulation of new competitors. Nonetheless, incumbent phone companies remain subject to rate regulation for many of their services at both the federal and the state levels.

The advent of VoIP challenges the dual federal/state regulatory framework in two respects. First, VoIP can make it difficult to determine the beginning and end points of a call, which is the normal way of telling whether a call is interstate or intrastate. A VoIP customer can obtain a local phone number using an area code from a distant state. For example, a customer living in Washington, D.C., who has family in Los Angeles could purchase a 213 number from a VoIP provider so her relatives do not need to pay for a long-distance call. Moreover, many VoIP services are nomadic, meaning that a customer can bring her phone number

with her when traveling. In the 2004 *Vonage Order*, the FCC held that this inability to determine jurisdiction supported "preemption"—that is, an assertion by the FCC of exclusive authority over rate regulation and market entry for VoIP providers, even where VoIP is used to make intrastate calls. That decision has been challenged in court, but it is not likely to be overturned on appeal.

Second, and more fundamentally, VoIP creates platform-independent competition. VoIP is an application riding over an IP network. As a result, it can be provided over any broadband facility, including DSL, fiber, cable, and

▶

wireless. As long as the network owner does not limit users' access to applications—which the FCC has made clear it will not tolerate, at least when the telephone company is the network owner—any potential provider can offer VoIP to any potential customer. Given the prospect for widespread local phone competition from cable companies, independent providers such as Vonage and Skype, fixed and mobile wireless carriers, and information service providers, it is not clear that *any* regulation of phone rates and market entry remains necessary at the state level. In fact, regulation of the incumbent phone company's rates is likely to be counterproductive: There is little risk that the incumbent's rates will be set too high, because competition will discipline above-cost rates. But if regulators set the incumbent's rates too low, they will forestall competitive entry.

Recognizing this fact, some state regulators have begun to reduce their regulation of the incumbent carrier's rates. Although that trend is likely to continue, many states may be reluctant to give up their regulatory authority. At some point, therefore, legislative change may be needed to assure that residual rate regulation does not stand in the way of additional broadband deployment.

Of course, state regulation is not likely to disappear. Rather, states will continue to play an important role in ensuring access to e911 and protecting consumers from unscrupulous competitors. The latter function, however, may be subsumed within general consumer protection laws, since there may not be a need for communications industry–specific rules.

## Reform of Inter-Carrier Compensation

Inter-carrier compensation refers to payments made by one service provider to another when traffic is exchanged between the two companies. It is difficult to imagine a more arbitrary system of inter-carrier compensation than what exists today. Even where the same exact facilities are used to originate and terminate calls, the level of compensation and the direction of payment depend on the identity of the interconnecting service provider:

• When two local phone companies exchange a local call, the originating carrier pays the terminating carrier a rate that is usually less than one-tenth of a cent per minute.

• When a local phone company originates or terminates a long-distance call, the long-distance provider pays "access charges" to the local phone company at a rate ranging from one-half to several cents per minute, depending on the size of the phone company and whether the call is intrastate or interstate.

• When a local phone company and a wireless carrier exchange traffic, the terminating carrier receives compensation if the call is "local." But in the wireless context, "local" is defined more broadly than in the wireline context to include an entire Metropolitan Statistical Area (MSA).

• When an information service provider interconnects with a local phone company, it neither pays nor receives per-call compensation. Rather, it buys either a business line or an ISDN connection, and it does not pay access charges, even if it uses that connection to originate and terminate long-distance calls.

This system creates powerful incentives to engage in arbitrage—for example, by characterizing traffic as interstate rather than intrastate (because interstate access charges are lower) or by classifying a call as an information service rather than a telecommunications services (to avoid access charges entirely). The advent of VoIP threatens to undermine the inter-carrier compensation system altogether. Not only is it hard to determine the jurisdictional nature of VoIP calls, but also many parties have asked the FCC to find that VoIP is an information service and thus exempt from access charges. If that position is upheld, then access charge revenues could be decimated as VoIP accounts for an ever greater proportion of voice calls. This is a serious concern for local phone companies, particularly in rural areas, which use those revenues to support the maintenance and operation of their networks.

Reforming inter-carrier compensation may be the most intractable problem facing the FCC because so much money is involved. Any fundamental change to the system could cause a marked shift in revenues and payment obligations. Further complicating things, inter-carrier compensation reform must govern both interstate and intrastate traffic, but the FCC likely lacks jurisdiction to dictate rules for intrastate traffic. As a result, Congress may need to get involved.

In the meantime, expect the FCC to try to minimize the irrationality of the current system. In particular, it may require VoIP providers to pay some compensation for their use of local phone networks. The FCC also may adopt a "unified" terminating compensation rate for the exchange

of all forms of traffic—or at least all interstate traffic. That rate is likely to be lower than current access charges (at least for the nonrural phone companies), in which case users may see some increase in the subscriber line charge (or a new flat charge). Given the difficulty of these issues and the fact that there will not be a full complement of FCC commissioners until later this year, it is not likely that any changes will be made until early to mid-2006.

## Universal Service Reform

Related to inter-carrier compensation reform is the need to stabilize universal service support. Although universal service has been a national policy since the early days of the Bell System, Congress formalized the concept in Section 254 of the Communications Act, which states that all Americans should have access to affordable, high-quality phone service.

Before passage of the 1996 act, universal service was funded largely through implicit subsidies. For example, access charges, business rates, and vertical feature rates were set above cost in order to help support below-cost residential service. With the advent of local competition, these implicit subsidies became untenable. Accordingly, Congress directed that universal service support

(at least at the federal level) be explicit, specific, and predictable.

In response, the FCC required all telecommunications providers to contribute a percentage of their interstate revenues to a federal universal service fund. (Several states have established similar funds.) Over time, the federal fund has grown while the revenue base has shrunk. Fund growth has been driven by implementation of the schools and libraries program (the "E-rate" mechanism) in the late 1990s and the eligibility of competitors to receive high-cost support in rural areas. The revenue

base has diminished because landline long-distance minutes have been replaced by wireless usage and, increasingly, VoIP. The unhappy result for end users has been a doubling of the amount they have to pay into the fund (as a pass-through from their service providers) over the past four years.

The FCC has been considering ways to modify the universal service rules to ensure sufficient funding going forward. Once again, the rise of VoIP is making reform even more urgent. If VoIP revenues are not included in the contribution base—for example, if
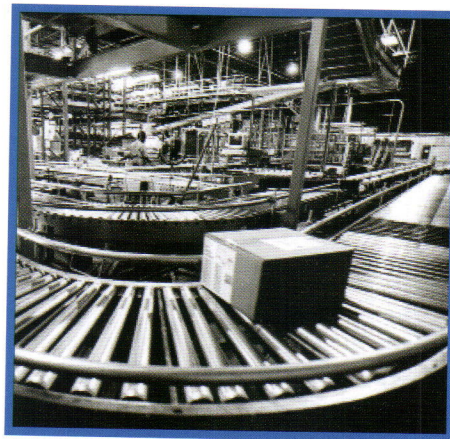
▶

VoIP is considered an information service—then the contribution percentage will continue spiraling upward. In response, the FCC may assess contributions based on phone numbers rather than revenues. Doing so would result in a more stable contribution base, but it would also raise troubling questions for ACUTA members.

For example, the FCC would need to distinguish between "assigned" and "working" numbers. Many ACUTA members have blocks of numbers, only some of which are in use (i.e., working) at a particular time. In addition, number use at colleges and universities is seasonal; in the summer, numbers assigned to students may be non-working. Assessing universal service charges on all numbers, instead of just working numbers, could cause a tremendous increase in ACUTA members' phone bills.

The FCC also needs to make sure that assessing contributions on the basis of phone numbers does not trigger inefficient changes in usage patterns or technology. For example, ACUTA has noted that assessing numbers might lead customers to discontinue use of DID numbers or to switch to IP services that use ENUM resources. Likewise, assessing DS1s, DS3s, and OCn facilities based on an overly aggressive assumption about the number of voice channels carried on those lines could dissuade customers from deploying higher-capacity circuits.

The FCC probably will act on the universal service reform proposal in the fall. Nonetheless, the new rules may not take effect for at least 9 to 12 months to give the industry time to adjust back-office systems to accommodate the shift to a number-based contribution mechanism.

## Conclusion

Incremental change in telecommunications policy is no longer sustainable, and VoIP is the agent for revolution. Ultimately, ACUTA members should benefit from the new regulatory environment, which should promote greater competition and more rapid deployment of broadband technologies. As with any revolutionary change, however, the transition will be disruptive and confusing. Of course, that's nothing new for telecommunications professionals.

Jeff Linder is a partner in the Washington, D.C., law firm of Wiley Rein & Fielding and is a frequent speaker and active participant in ACUTA. Reach Jeff at jlinder@wrf.com.

# Publish Your Story in the *ACUTA Journal*
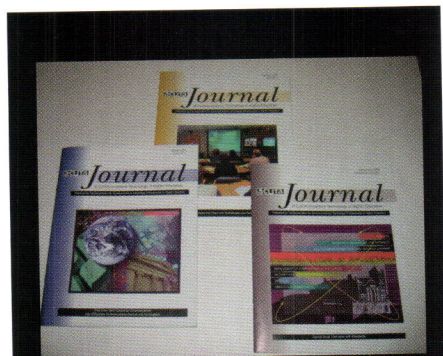
## 2006 Editorial Calendar

Spring:  Best Business Practices: Improving the Bottom Line

Summer: Meeting the Security Challenge

Fall:    Infrastructure: The Building Blocks of Communications

Winter:  Broadband Access: Supporting Students, Faculty, and Staff

Does your department or your campus have a story to tell? Have you completed a project, installed a new system, solved an old problem, come through a crisis, or formulated a solution to a situation you thought would never go away?

If so, your peers—our readers—want to hear from you!

### Some Benefits of Writing

Writing for the *ACUTA Journal* provides excellent visibility for your campus or your department. When you share the details of that complex project you just completed or a new revenue-generating idea, you give some well-deserved recognition to your staff, reveal your personal leadership skills, and, at the same time, give other members some ideas that may prove useful on their own campus.

We also pay a $50 honorarium to our members whose articles are published. (It's not a lot, but your mother will be so proud!)

### Here's All You Do

1. Read the articles in this or another recent *Journal* to get familiar with the style and depth of content.

2. Submit your idea for a story to Pat Scott, ACUTA communications manager, via e-mail (pscott@acuta.org) or fax (859/278-3268).

3. With or without help from staff or a freelance writer, put your story together and submit it about 4 months prior to the mail date of the issue you'd like to be in.

4. Pat will review it and get back to you with any questions or suggestions.

5. Wait to see your work in print!

Stories in the *Journal* are typically 1,500 to 2,500 words in length. Graphics, photos, and illustrations are a nice addition, but not usually essential.

*Call today: 859/278-3338, ext. 221. You could be a published author, too!*

# Report from the FCC CAC

Tamara Closs

Duke University

## FCC CAC Working Groups & Chairs

Disability Access
Deaf and Hard of Hearing Consumer
Advocacy Network
Claude Stout

Telecommunications Relay Service
Hamilton Relay
Dixie Ziegler

Consumer Affairs & Outreach
Consumers First
Jim Conran

Rural and Underserved Populations
Telecommunity Resource Center
Gene Crick

Advanced Technologies
Media Access Group, WGBH
Larry Goldberg

Homeland Security
EAD & Associates
Elizabeth Davis

Competition Policy
AARP
Debra Berlyn

Media
Democracy Now!
Denis Moynihan

The FCC Consumer Advisory Committee (CAC) was established in 2000 for the purpose of making recommendations regarding consumer issues within the jurisdiction of the Commission and to facilitate the participation of consumers (including people with disabilities and underserved populations, such as American Indians and persons living in rural areas) in proceedings before the Commission. The Commission began its new session June 10, 2005, with 55 new and returning members in attendance. This is the first time ACUTA, or any higher-education association, has had an appointed member. A list of the members and other detailed information can be found at http://www.fcc.gov/cgb/cac/.

The June 10 meeting had a very full agenda, and the meeting itself was quite interactive. Shirley Rooker from Call for Action and chair of the FCC CAC called the meeting to order, and Scott Marshall, CAC designated federal officer, provided meeting logistics. The chair and commissioners were invited for introductions, hosted by Monica Desai, chief, Consumer and Governmental Affairs Bureau. Commissioner Jonathan Adelstein spoke and had a very pro-broadband-to-rural-communities message.

Commissioner Michael Copps could not attend but sent a letter encouraging all of us to be active, engage in debate, and work toward common-ground solutions but to feel comfortable offering a minority report.

Chairman Kevin Martin also spoke to us, commending the past work of the CAC and explaining expectations for the future of the committee. Jay Keithley, deputy chief, policy, CGB, provided an overview of issues pending before the Commission of interest to consumers.

In between the introductions of these representatives, the appointed committee members introduced themselves.

In the afternoon, our responsibilities and the processes and procedures were explained to us. Then we arrived at the focus of the meeting—establishing working groups, where the work of the CAC is done. The first step was to determine the scope of each working group. Returning members were very helpful in recognizing that some of the previous working groups were too broad and certain deserving topics were not closely reviewed. We were advised that if, in the course of our work, we determine that a separate working group needs to be established, we have the flexibility to take such action. This process took a lot of time but was very informative in helping us understand the broad array of topics to be researched.

The next step was to assign members to the work groups. After previous discussion with the ACUTA Board and legal counsel, I volunteered for Advanced Technologies and Homeland Security work groups. At the left is the final list of the working groups and chairs.

A primary goal of ACUTA's new strategic plan is public policy: "Public policy and regulatory reform will be enacted that provides a positive communications environment for higher education and the constituencies it serves." To be effective in this strategy requires an increased level of interaction with FCC and other federal agencies, and this is a giant step toward achieving the goal. The next full CAC meeting is November 18, 2005.

▼

# The USA Patriot Act in 2005:
# What Technology Leaders Need to Know

Michael Corn

Peter M. Siegel

University of Illinois

Urbana-Champaign

With the passage of the USA Patriot Act in October 2001, many universities were forced to examine in detail their procedures for participating in law enforcement investigations of computer- and network-related intrusions. Some had never formalized these procedures or, at a minimum, found themselves exposing what had essentially been internal activities to public scrutiny for the first time. As the debate over the renewal of the Patriot Act becomes energized, it is important to consider not just our views as citizens, but also how we as technology and campus leaders respond to investigations. Most importantly, we must consider how to organize our responses in advance, so that we can serve our institutions most effectively.

Institutions must adopt a posture of readiness with regard to law enforcement investigations in order to be equipped for the consequences of the Patriot Act. Whatever your personal views, an ad hoc, reactive, or disengaged approach is likely to increase the negative impact on your campus community in terms of disruption of services or concerns about privacy. This article presents policy, effective procedures, and a healthy working relationship with law enforcement as the essential elements of this institutional posture. (For a substantive analysis of the Patriot Act and its importance for universities, as well as pointers to other materials, we recommend Tracy Mitrano's "Potential Implications for Information Technologies in Colleges and Universities," available at http://www.cit.cornell.edu/oit/PatriotAct /present.html.)

### The Patriot Act in Context

While the legal and philosophical dimensions of the Patriot Act are profound, at a practical level the act really has not significantly changed how we operate. What has dramatically changed is the frequency of computer- and network-related intrusions that require legal or other investigation. In addition, the number of such investigations instigated by external agencies has notably increased. Even before the Patriot Act, you could be required to disclose information through warrants, subpoenas, and court orders; similarly, you could be legally compelled to maintain confidentiality regarding the nature or even the existence of an investigation. Under the Patriot Act, the FBI still must submit subpoena requests to a federal judge.

The Patriot Act as currently written does, however, significantly lower the degree of oversight inherent in many situations, and it increases surveillance and investigative powers of law enforcement agencies. In addition, it does the following:

- Allows searches without notification for an undefined "reasonable period"

- Extends the metaphor of phone taps to the electronic media (e.g., networks, computers) in addressing terrorism

- Trumps Family Educational Rights and Privacy Act (FERPA) and other privacy acts of import to universities

- Can require complete confidentiality, even preventing disclosure of existence or nature of investigations

- Can require preserving data up to 180 days

- Allows voluntary emergency disclosure by concerned citizens

However, despite misconceptions to the contrary, the Patriot Act does not obligate an institution or individual to preserve specific information, authentication, or network-access logs, for example, for any particular length of time, unless such preservation is expressly requested. Similarly, the Patriot Act includes no "design mandate" specifying a requirement for designing a tapping mechanism into your network or system architecture. However, information you may have maintained by accident or "just in case" may need to be restored and provided as part of an ongoing investigation, sometimes through considerable effort or expense. In addition, the Patriot Act expressly forbids the use of a tap against a U.S. citizen "conducted solely upon the basis of activities protected by the first Amendment to the Constitution."[1]

The Patriot Act does change how an institution needs to prepare to interact with law enforcement; however, when examined in depth, the financial impact of this change is quite minor, though the cultural impact may present some initial challenges to all of us. By having in place effective and transparent procedures, strong policies, and an excellent working relationship with law enforcement, any investigation engaging law enforcement will be strengthened, and investigations pertaining to national security will have a minimally disruptive effect on the institution.

Let's review the three key mechanisms for effective preparation: policy, procedure, and working with law enforcement.

### Policy

All effective operational procedures must be grounded in policy. Clear policies with regard to the release of confidential information or access to electronic data will shape the discussion surrounding these issues. For most members of your community, these discussions will define the boundaries of their participation in any law enforcement investigation.

At the University of Illinois at Urbana-Champaign (UIUC), our Acceptable Use Policy specifically addresses not only who can approve a request for access to electronic data but also who is authorized to request access, the procedures for notifying the individuals whose data is being requested, and the conditions that must be met before disclosure is provided.[2] In effect, this section of the policy is a kind of sunshine law that exposes to the campus community the inner workings by which access to electronic data is granted. Just as important, our policy has been reviewed and endorsed by the UIUC campus senate, providing an essential socialization process well worth the investment.   ▶

When developing your policies on data retention (e.g., logs, backups) be sure to consider the "mosaic effect," that is, the ability to connect seemingly disparate information into a cogent whole. For example, building- or door-access records could be combined with authentication records from a shared computing lab to associate an individual with particular Web browsing behaviors. The goal here is not to thwart legitimate investigations, but rather to ensure that privacy is not inadvertently violated. More to the point, such information could be used by hackers for identity theft or for other truly disruptive activities.

## Roles and Issues to Consider to Build Effective Procedures

In order to ensure that neither personal privacy nor the integrity of any investigation is compromised, all law enforcement investigations should be kept as limited and, therefore, as confidential as possible. While certain classes of investigations may require this, establishing clear and well-understood roles for investigations is the only effective way to ensure confidentiality. The critical roles needed are the following:

• Legal Counsel

Your campus legal counsel should be intimately familiar with your campus policies and also needs to take responsibility for interpreting any formal requests for information that arrive on campus, as well as verifying their applicability to your environment. It is they, not your security analyst, who need to clarify legal responsibilities for privacy and compliance.

• IT Security

The head of your campus IT security has two roles; First is to act as the party responsible for providing requested

information acquired from centrally maintained systems. In the highly distributed computing environment of the modern campus, he or she should be able to identify and interact with the minimal number of individuals within campus units who may need to be approached to obtain requested information. In addition, he or she should have the skills and tools necessary to acquire and preserve electronic evidence.

• Campus/Local Law Enforcement

In many cases, particularly those involving the physical acquisition of equipment, the presence of campus or local law enforcement agents is essential. Beyond this they have established procedures for validating the credentials of other law enforcement agents who may present themselves to the campus. When an internal investigation needs escalation to state or federal law enforcement, your local or campus police will always have established contacts and be able to assist.

Beyond identifying individuals at your institution to fill these roles, you and your colleagues must develop standard procedures for responding to requests for information and should begin by meeting regularly to address questions such as these:

• When a subpoena, national security letter, or similar document arrives, who can review whether the requested information exists, how long it will take to collect, or how voluminous it is?

• If the information requested is suspected to exist in a server maintained by a department, who should be contacted in that department? The server administrator? The unit head? Who can judge the likelihood that a given individual can adhere to the required degree of confidentiality? Who

should do the contacting?

• If an investigation exposes the presence of compromised computers on your campus, how can the institution protect itself without undermining the investigation?

• Who serves as backup in each of the established roles if someone is unavailable or on vacation?

It's important to develop these procedures before a major incident occurs and, more importantly, to develop good working relationships with law enforcement over a period of time. Since you are working across cultural boundaries, even within the university, trust and an appreciation of mutual competence and common interest take time to develop.

## Law Enforcement Relationship

While all of the above procedures are relevant to almost every significant internal investigation, they are particularly critical for establishing a relationship built on trust with law enforcement. This relationship can help bridge the gap between legislative paradigms and the reality of the modern large data network. For example, though it is common to use the metaphor of the "wiretap" with reference to data networks when discussing the Patriot Act, in practice, this image breaks down quite quickly.

At UIUC, the campus network (UIUCnet) hosts upward of 55,000 computers, sees approximately a terabyte of traffic per day at the campus border, and typically delivers up to one million e-mail messages per day. Our campus exit-flow logs alone grow at the rate of one gigabyte per hour. The logistical difficulties of "tapping" this data stream are prohibitive, to say nothing of the technical skills and tools that would be necessary to make sense

of it. Even acquiring information when it can be restricted to a small subset requires intimate knowledge of the campus network topology and the individuals who maintain portions of it.

Consequently, it is important to do the following:

• Work closely with law enforcement to educate them about what you can and can't provide. For example, our central e-mail system is backed up nightly. That snapshot only reflects the state of the system at the time of the backup. We simply cannot provide a complete copy of all the e-mail sent to and from a particular account.

• Be explicit and honest about the impact on operations a given request could have. Sticking with our e-mail system example, we snapshot the entire system for the backup process. Consequently, restoring a backup requires building a system with the same OS patch level as that which existed at the time of the backup and restoring the entire e-mail system (~111,000 accounts). This is not a process that can be done instantly and could, if requested in an emergency, require pulling staff from operational duties.

• Work with the agents involved in the request to ensure they're asking for no more than what they really need. It is quite common to find that the agents are working at the very edge of their technical knowledge. You can help them understand precisely what information will assist their investigation and what would only burden it. That is, by working with the agent, you will usually be able to narrow the scope of the request, thus minimizing the impact of the request on your university, the agent, and the privacy of the parties involved. As a side benefit, limiting the information in this way can ensure that the information is not inadvertently shared with parties unrelated to the investigation.

## Conclusion

In conclusion, it is important to recognize that while the Patriot Act may add to an already complex picture regarding computer security, you are in a strong position to protect the interests of your campus community by taking a proactive, thoughtful approach to law enforcement investigations. If members of your community have concerns, we can encourage them to air these as part of public, academic discussions, clearly separated from any actual investigations. While your campus police or legal counsel may officially be in leadership roles, you must be at the table not only to define the most effective internal processes during an investigation, but also to ensure that the right information is maintained throughout the university. Given the increasing number of intrusion incidents, clear policies, well-vetted procedures, strong internal partnerships, and a constructive relationship with law enforcement are not luxuries—your faculty, students, and staff are depending on you.

### References

[1] Sec. 214.a.(2).

[2] http://www.fs.uiuc.edu/cam/CAM/viii/viii-1.1.html

Peter M. Siegel is chief information officer at the University of Illinois at Urbana-Champaign. He can be reached at psiegel@uiuc.edu. Michael Corn is director of security services and information privacy at UIUC. He can be reached at mcorn@uiuc.edu.

# Universal Service Funding in a Changing Telecommunications World

Andrew Isar
The Northridge Group

Recent changes in the telecommunications industry, including the maturation and further proliferation of new technologies such as VoIP, and expanding availability of high-speed broadband connectivity, have obvious impacts on institutional and residential telecom subscribers. These tectonic industry shifts introduce myriad subtle impacts— even on seemingly unaffected users in the universal service and universal service funding arenas.

## Universal Service Funding

The concept of universal service was born out of historic public policy objectives to ensure that all Americans retained access to basic telecommunications services regardless of their ability to pay for it or the cost of providing service to them. To achieve the goal of universal service, federal funding was established to subsidize the cost of providing service to certain low-income subscribers, educational institutions, and healthcare facilities and those people located in less densely populated, insular rural areas where network service costs could otherwise prove prohibitive for end users. Several states also established state universal service funding programs to supplement or replace federal funds.

At the federal level, universal service funding is governed by the statutory framework established in the Communications Act of 1934, as amended by the Communications Act of 1996 (the "Act"). Pursuant to Section 254(d) of the act, "[e]very telecommunications carrier that provides interstate telecommunications services shall contribute, on an equitable and nondiscriminatory basis, to the specific, predictable, and sufficient mechanisms established by the Federal Communications Commission to preserve and advance universal service."[1] The FCC subsequently adopted the additional principle that federal support mechanisms should be competitively neutral, neither unfairly advantaging nor disadvantaging particular service providers or technologies.[2] Prior to adoption of the Telecommunications Act of 1996, universal service was achieved largely through implicit support mechanisms.[3]

## Contribution Methodology

Federal carrier universal service fund contributions are assessed on gross-billed end-user domestic interstate and international telecommunications service revenues. Generally, any entity which provides a telecommunications service as defined,[4] is subject to universal service fund contributions, to the extent that the calculated contributions exceed $10,000.00 annually.[5] The FCC does not impose a mandatory end-user surcharge for recovery of universal service contributions by telecommunications providers, but instead allows contributors to determine how to recover universal service contributions from their customers. The FCC requires only that contributors not shift more than an equitable share of their contributions to any subscriber and that contributors "provide accurate, truthful, and complete information regarding the nature of the charge."[6]

## Universal Service Funding Success and Growth

Universal service funding has been effective in achieving program objectives of increasing telephone service availability across the country, achieving peak penetration of 95.5 percent in March 2003.[77]

To drive such high penetration, universal service fund program disbursements have steadily increased each year, yet the base of contributing carrier revenues on which universal service funding is based has declined from a high of $21 billion in 2000 to $16.5 billion by the end of 2004.[8] These factors have contributed to the growing concern over future program funding.

Major changes looming in the telecommunications industry at a time of growing funding demands and declining contributions, however, have ominous implications for the future of universal service funding and the telecommunications service end users who ultimately fund universal service.

## The Winds of Change

Federal and state funding programs have been effective in promoting universal service in part because funding sources—telecommunications carriers and their customers—and program administrative costs historically remained relative constants. The advent of voice over Internet Protocol (VoIP) technology as an alternative communications medium, the potential broadening of "basic" telecommunications services to include high-speed broadband services funded by the universal service program, the reduction in contributors, and growing pressure on universal service funding, have conspired to exacerbate the alarming gap between funding demands and contributions.

## VoIP Telephony

VoIP telephony is perhaps the most feared immediate threat to universal service funding. The reason is fairly simple—VoIP telephony services stand to eclipse conventional telecommunications service usage in the relatively near future, and VoIP service providers are not currently required to contribute to universal service funds. If VoIP telephony services remain exempt from universal service funding contributions, the level of contributions will fall precipitously while fund requirements will continue to rise. This will lead to a funding crisis that will be shared by an ever-diminishing number of contributors, and will be felt disproportionately by larger telecommunications service subscribers, including colleges and universities.

Although VoIP telephony technology has been with us for nearly a decade, the technology was, until recently, viewed as a novel and technologically inferior method of communication. Its existence had no commercial impact, and therefore posed no threat to universal service fund programs. VoIP's growing commercial appeal as an "all you can talk" flat rate substitute for conventional long-distance telecommunications services quickly changed all that.

▶

Over the past three-plus years, a host of new VoIP telephony providers, including high-profile companies such as Vonage Holdings Corp., Skype, and 8x8, introduced VoIP telephony services commercially. But in the initial stages of a VoIP telephony market, the number of subscribers these and other providers attracted constituted only a tiny fraction of the total number of telecommunications subscribers and universal service fund contributors. In addition, virtually all initial VoIP telephony subscribers were residential users who accepted the technologically inferior service as a money-saving supplement to their existing service providers.

As technology has improved, VoIP telephony has been steadilygaining market acceptance, and providers have become more aggressive in selling VoIP telephony. As a result, an increasing number of residential and commercial enterprises are utilizing VoIP telephony as a replacement for, rather than a supplement to, conventional voice services. On June 1, Vonage chief executive officer Jeffrey Citron claimed that his company would hit the one million–subscriber mark by year's end. He noted that Vonage currently serves more than 700,000 subscribers and is adding approximately 15,000 new subscribers a week. Vonage added 249,000 subscribers in the first quarter of 2005, up from 114,000 in the fourth quarter of 2004.[9]  These numbers tell a compelling story about rapidly diminishing universal service fund contributions under the current regulatory regime, and regulators have taken note.

The potential impact of VoIP telephony on universal service funding has not been lost on the Federal Communications Commission. In a 1998 report to Congress regarding VoIP telephony and universal service, the

FCC for the first time considered the proper classification of emerging VoIP telephony services within the narrow context of universal service funding.[10] At that time, the FCC concluded that "[c]ertain 'phone-to-phone [Internet protocol] telephony' services lack the characteristics that would render them 'information services' … and instead bear the characteristics of (regulated) 'telecommunications services.'" Yet having reached that conclusion, the FCC was not yet ready to subject VoIP telephony to full regulation, leaving itself several "outs." Moreover, the FCC concluded that VoIP telephony did not (then) threaten universal service, stressing that it was not appropriate to make any definitive pronouncements "in the absence of a more complete record focused on individual service offerings."[11]

But the FCC planted some regulatory seeds by affirmatively determining that some forms of "phone-to-phone IP telephony are 'telecommunications,' and that to the extent that providers offer such services to the public for a fee," they would be subject to universal service fund payments. The FCC reasoned that "if such providers are exempt from universal service fund contribution requirements, users and carriers will have the incentive to modify networks to shift traffic to Internet protocol and thereby avoid paying into the universal service fund or, in the near term, the universal service contributions embedded in interstate access charges. If that occurs, it could increase the burden on a more limited set of companies still required to contribute." This pronouncement captures the essence of concerns over VoIP telephony and universal service funding.

The FCC has walked a fine line between (1) keeping Internet protocol-

based applications, including VoIP telephony, relatively unencumbered by regulation in an effort to promote their development as a matter of public policy and (2) ensuring that new technologies, such as VoIP telephony, do not upset other public policy objectives such as universal service. On March 10, 2004, the FCC released a long-awaited Notice of Proposed Rulemaking ("NPRM") regarding VoIP, more generically termed IP-enabled services.[12]  The NPRM solicited comment on a broad range of regulatory issues surrounding IP-enabled services, including universal service contributions, while providing preliminary FCC thinking on how the FCC might approach IP-enabled service regulation. Among the issues raised by the FCC was whether the FCC retained authority to require VoIP providers to contribute to universal service as "information service" providers. The FCC also sought comment on the interplay between information and telecommunications services for purposes of fund assessment and the methodology for imposing assessments on providers based on telephone number utilization or connectivity, the latter for high-speed broadband service providers. Action on the FCC's NPRM and the universal service fund issues it raises remains pending.

On November 10, 2004, the FCC ruled in a separate proceeding that VoIP telephony services that utilize the public switched network are jurisdictionally interstate and under the exclusive purview of the FCC.[13]  This finding expressly forecloses state jurisdiction over VoIP telephony services and, for now, the ability of states to impose universal service contribution obligations on VoIP telephony providers, unless pending

appeals overturn the decision. The FCC elected not to determine whether VoIP services are to remain unregulated information services or regulated telecommunications services, distinctions that could impact how—or potentially if—VoIP telephony service providers and their users would contribute to universal service funding. Of the ruling, the Consumers Union recently stated that decision threatened universal service funding, noting, "State universal service programs are also at risk after a recent federal ruling which prohibits states from imposing universal service fees on 'voice over Internet' phone service."[14]

The proliferation of VoIP providers raises another potential funding wrinkle—the specter of universal service funding for VoIP providers. Pursuant to Section 214(e) of the Act[15] and Part 54 of the FCC rules, entities deemed Eligible Telecommunications Carrier (ETC) may draw from universal service funds. ETCs must maintain their own network facilities and demonstrate to state regulators that they provide the minimum services designated for universal servicefunding

under FCC rules.[16] Although the chances of a VoIP provider drawing from universal service funding as an ETC are currently negligible at best, it may become increasingly possible for VoIP providers to gain ETC status in the future as successful VoIP providers deploy their own networks and target less competitive, rural markets. We have already witnessed a growing number of wireless providers, such as Western Wireless, who have mastered the ETC process for the rural areas they serve and generated millions of universal service fund dollars.

For now at least, the matter of whether VoIP providers will be subject to universal service contributions remains unanswered and will likely be so for some time as the FCC grapples with the issue of whether VoIP services are regulated "telecommunications services," unregulated "information services," or a regulatory hybrid that could contribute to universal service funding.

### Broadband.[17]

High-speed Internet connectivity is viewed as an engine that will drive

economic development, particularly in rural areas.[18] According to the FCC, broadband access is not yet ubiquitous, deployment costs remain high, and access is limited in underserved areas.[19] To that end, one of the FCC's policy objectives is to "promote the availability of broadband to all Americans." FCC statistics indicate that "the number of residential and small business subscribers to high-speed services has more than tripled during the same period, from 7.8 million lines in June 2001 to 26 million lines in December 2003."[20]

Congress, too, has readily embraced the promise of broadband availability. In a June 28, 2005, letter addressed to The House Committee on Energy and Commerce[21] Chairman Joe Barton and Ranking Member John Dingell, more than sixty House representatives stressed that "[A]s the United States moves into the broadband age, it is imperative that we do not forget the [universal service] principles that have served us so well. Let's make sure that commitment to universal access to communications services is protected during the re-write so that all Ameri-

cans can have access to advanced [broadband] communications, such as DSL, cable, wireless, and satellite."[22] The implications that broadband services should be subsidized through universal service funding under Section 254 as a matter of public policy are clear. Inclusion of broadband universal service fund subsidies stand to add yet uncounted millions to universal service funding without a readily identifiable source for added funding.
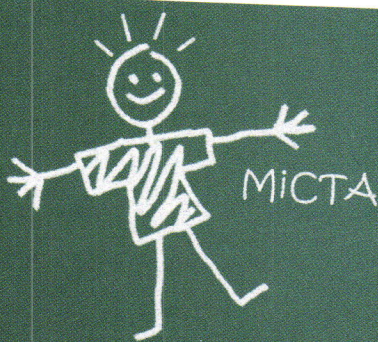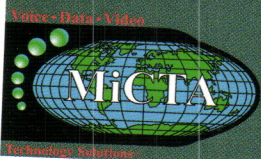
### De Minimis Providers

The Section 54. 708 exemption of de minimis providers, those whose calculated annual universal service contribution amounts are less than $10,000, further exacerbates the pressures on universal service funding. Although the number of competitive telecommunications service providers may increase, so long as these providers are exempt from contribution obligations, any increase in the number of providers does not guarantee an increase in contributions. Arguably, even if VoIP providers were ultimately mandated to contribute to universal service funding, the number of VoIP contributing companies would likely remain few if the de minimis exception applied.

### Is the Universal Service Fund Broken?

The federal universal service fund program has undergone numerous changes since its inception, resulting in a highly complex system of subsidies and funding. Allegations of waste, fraud, and abuse have also arisen, most recently regarding mismanagement of the Schools and Libraries Universal Service Support Mechanism. On June 14, 2005, the FCC initiated a broad inquiry into the management and administration of the fund, as well as

how to further deter waste, fraud, and abuse. [23] The FCC initiated this procedure to address alleged inefficiencies and fraud, which also have profound impacts on funding requirements and, therefore, on the level of funding contributions.[24]

Allegations of program mismanagement, if true, have serious implications

> If the contribution factor were passed through directly to end users, a medium-sized institutional end user's universal service fund contribution on a $7,000,000 per year telephone bill could increase $56,000, from $714,000 to $770,000.

for the continued growth in funding requirements and the resultant costs borne by telecommunications users. Moreover, a comprehensive reengineering of the universal service fund regime has become readily apparent to keep up with mounting pressures on contributions and funding.

### The Future of Universal Service Funding— Where Is It headed?

A detailed analysis is not required to conclude that telecommunications users stand to continue assuming an increasing financial burden for

maintaining universal service public policy objectives at current levels, in the absence of fundamental regulatory changes. For example, under the FCC's current 3Q05 universal service contribution factor calculations, carriers will contribute at the rate of 10.2 percent of domestic interstate and international revenues.[25] Presuming program requirements rose by 3 percent and the contribution base decreased by 5 percent due to end-user migration to VoIP, the contribution factor would rise to 11 percent. If the contribution factor were passed through directly to end users, a medium-sized institutional end user's universal service fund contribution on a $7,000,000 per year telephone bill could increase $56,000, from $714,000 to $770,000.

The siphoning of telecommunications users away from conventional universal service fund–contributing subscribers to VoIP telephony, as VoIP telephony becomes a "main stream" telecommunications medium, will substantially reduce universal service fund contributions so long as VoIP providers are not required to contribute. Funding gaps will have to be made up by greater contributions from the existing base of contributors.

Yet it is unlikely that VoIP telephony providers and their customers will withstand pressure to impose universal service fund contribution obligations on VoIP telephony services. What remains to be seen is when VoIP telephony providers will likely have to begin contributing to the fund and how much. One potential scenario would have VoIP providers contribute less based on differences in technology between IP-enabled technology and conventional telecommunications media. If providers of VoIP telephony

services are subject to lower contribution levels, the outcome may still result in higher universal service fund contributions from conventional telecommunications users, although not as pronounced as if VoIP telephony users continued to escape contributions altogether. The "VoIP factor" on universal service funding warrants careful attention by institutional telecommunications managers, even if they have no immediate interest in VoIP technology.

And what of program policy objectives and administration? If past is prolog, we can anticipate that the demands on universal service funding will increase commensurate with population increases and an emphasis on broadband accessibility, if public policy objectives remain unchanged. We need only look at historic funding trends to see that we will not escape higher funding needs, presuming existing public policy objectives are retained. Changes in fund administration may prevent program waste, fraud, and abuse, but arguably not enough to be felt by fund contributors.

**"Something has to give."**

Even under a reengineered universal service funding paradigm, there will be contributors and recipients of funding for "basic" services. How each of these elements of universal service funding are defined will ultimately determine who contributes for what and how much. By more fully understanding the interrelationship between universal service funding policy, programs, and the impact of technology on universal service funding, institutional telecommunications managers can anticipate changes that will impact the cost of telecommunications services, if not actively participate in the process of shaping future universal service fund policy.

Andrew Isar is a consultant affiliated with The Northridge Group, Inc., whose practice focuses primarily on telecommunications regulation and public policy. He may be contacted directly at aisar@northridgegroup.com.

## References

[1] 47 U.S.C. § 254(b).

[2] See Federal-State Joint Board on Universal Service, CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776, 8801-03, paras. 46-51 (1997), as corrected by Federal-State Joint Board on Universal Service, Erratum, CC Docket No. 96-45, FCC 97-157 (rel. June 4, 1997), and Erratum, 13 FCC Rcd 24493 (1997), aff'd in part, rev'd in part, remanded in part sub nom, Texas Office of Public Utility Counsel v. FCC, 183 F.3d 393 (5th Cir. 1999), cert. denied, 530 U.S. 1210 (2000), cert. dismissed, 531 U.S. 975 (2000) (Universal Service Order).

[3] See *Federal-State Joint Board on Universal Service,* CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776, 8784-85, ¶¶ 10-12 (1997) ("First Report and Order").

[4] Telecommunications" is the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." 47 C.F.R. §54.5.

[5] Termed "De Minimis" providers. Pursuant to Section 54.708 of the FCC's rules (47 C.F.R. § 54.708), telecommunications providers are not required to contribute to the universal service support mechanisms for a given year if their contribution for that year is less than $10,000.00.

[6] Id. 9199, para. 829.

[7] Industry Analysis and Technology Division, Wireline Competition Bureau, *Telephone Subscribership in the United States* (March 2005). *See* FCC *Trends in Telephone Service* (April 2005), Table 16.1

[8] Office of Management and Budget, Executive Office of the President, The Budget for Fiscal Year 2006, Historical Tables, Table 8-5: Outlays for Mandatory and Related Programs: 1962-2010, at 133-34 (2005) ("FY06 Federal Budget").

[9] *Information Week,* Small Business Pipeline (June 1, 2005)

[10] In the Matter of Federal-State Joint Board on Universal Service, CC Docket No. 96-45, FCC 98-67 (April 10, 1998) ["Report to Congress" also referred to as the "Stevens Report"].

[11] Id. 50.

[12] In the Matter of IP-Enabled Services, WC Docket No. 04-36, FCC 04-28 (Adopted February 12, 2004, rel. March 10, 2004).

[13] In the Matter of Vonage Holdings Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission, WC Docket 03-211, FCC 04-267, (November 10, 2004).

[14] Consumers Union, Universal Service—What's at Stake

[15] 47 U.S.C. §214(e).

[16] 47 C.F.R. §54.1 et seq.

[17] Operationally defined by the FCC as "services and facilities with an upstream (customer-to-provider) and downstream (provider-to-customer) transmission speed of 200 kbps or greater." See *Availability of Advanced Telecommunications Capability in the U.S., Fourth Report to Congress* (September 9, 2004).

[18] See e.g. FCC Strategic Goals. "The FCC's strategic goal for Broadband is to establish regulatory policies that promote competition, innovation, and investment in broadband services and facilities while monitoring progress toward the deployment of broadband services in the United States and abroad."

[19] Id. 10.

[20] Id.

[21] The Committee which will draft legislation to re-write the ill-fated Telecommunications Act of 1996.

[22] http://www.neca.org/wawatch/wwpdf/062905_15.pdf

[23] In the Matter of Comprehensive Review of Universal Service Fund Management, Administration, and Oversight, WC Docket No. 05-195 et al., Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking, FCC 05-124 (rel. June 14, 2005).

[24] "Our goal is to find ways to improve the program, both from the perspective of USF beneficiaries and from the perspective of safeguarding the fund itself. We recognize that some parties have raised concerns ranging from mismanagement to intentionally defrauding the program, and we take these concerns seriously." Id. 2.

[25] Based on universal service fund program requirements of $1.678657 billion and a contribution base of $16.524650 billion (0.101585 rounded to 0.102). See, i.e. FCC Public Notice, Proposed Third Quarter 2005 Universal Service Contribution Factor, DA 05-1664 (June 14, 2005).

▼

# Taking a Flier on Tower Lighting

Curt Harler

Contributing Editor

Often a college in a small town will have the tallest buildings around…sites that microwave and cellular providers crave. In an urban setting, a university's tall buildings are prime antenna placement locations. Both carriers and tower companies need those sites.

There is money to be made from entering a deal for antenna space with an outside vendor. Either the college can rent space directly to a carrier, or they can negotiate with a leasing company to sell the tower space for them.

In either case, there are legal responsibilities for marking the tower that must be met, whether the school is located in close proximity to an airport or sits out on the lone prairie.

We will look at the FAA regulations in a moment. But the first thing a college has to consider is whether they are legally responsible for meeting the regulations on the tower site. If the total height of the building plus the antenna tower is less than 200 feet, it is unlikely that there is any obligation. For anything above that, the regulations come thick and fast.

## Outsourcing Responsibility

"Just like maintaining photocopiers and other equipment, managing and marking towers usually falls outside a college's core expertise," says Jim Holmes, vice president and managing director of legal for Unison Site Management (New York, NY, http://www.unisonsite.com).

Any reader who wades through the FAA regulatory requirements below will appreciate the opportunity to off-load the

hassles onto someone else. However, the question remains, Who is responsible for meeting legal requirements: the college or the leaseholder?

According to the FAA, the responsibility for notifying the FAA and making all required changes rests with the person making the changes.

"The person or entity who is responsible for adding to the height of the building or tower, or who is adding a frequency, is the responsible party," says Rebecca Trexler, spokesperson for the FAA.

"If the tower is on a building or other structure that the owner wants to maintain ownership of, then the building owner is responsible to maintain lights, antennas, etc., unless the contract changes it," Holmes explains. This includes everything from the red lights to the red-and-white paint scheme to fences and gates.

A 20-story dorm building on a campus will already be lighted. If a telco or leasing firm wants to use the building to mount antennas, "The obligation will rest with the building owners, since they have a preexisting obligation to light it," Holmes says. In a case where the antenna is mounted on the side of the building, with no additional height, the responsibility almost certainly would remain with the college.

If a telco builds a 20-foot tower on top of the building, there could be a contractual transfer of the obligation to maintain the tower. "But the statutory obligation will remain with the building owner," Holmes states.

A different case would be where a company approaches the college to lease

land to put up a tall tower on a grassy knoll behind the stadium. "Philosophically, they came on board, and they would have to do the marking," Holmes says.

A third case might be where a university has a tower for the student FM radio station and cuts a deal to sell the tower and lease back space for $1 a year for college use. "In that case, if there is a transfer of the tower, the obligation for marking goes with the sale," Holmes says.

Obviously, it is a complicated process and one that the school's attorneys—not the facilities or telecom manager—should negotiate.

From a practical point of view, there likely would be a mixture of liability. But that depends on the state. In Louisiana, for example, the landowner is strictly liable for any accident, even if there is no way they could foresee it happening. Say a drunken student climbs a tower and falls. In most states, much would depend on whether a gate was left unlocked or other precautions were absent.

"Leases usually provide that—if I screw up, I fix it; if you screw up, you fix it," Holmes says. That includes liability for employees or others invited onto the property.

Towers do fall over. In that case, liability likely would be on the owner of the tower—unless a university groundskeeper had hit a guy wire with a tractor and caused the problem.

### FAA Tower Regulations

The FAA spells out its regulations for towers in painful governmentese. For starters, the FAA requires a full description of the structure, project, and so on, including all submitted frequencies and ERP. "Use exact information to clearly identify the nature of the project (e.g., microwave antenna tower; FM, AM, or TV antenna tower)," the FAA says.

You are required to specify the latitude, longitude, and height of each structure. When an obstruction evaluation study concerns an array of antennas or other multiple-type structures, specific information on each structure has to be included.

An aviation safety study is part of any new project. A marking and/or lighting recommendation is a required condition when aeronautical study discloses that the marking and/or lighting are necessary for aviation safety.

The FAA does concede that additions to an existing structure with no physical alteration to height or location (e.g., a side-mount antenna) where the structure was previously approved will accept that the recommended

▶

## Selling Out

If you have problems with a tower lease, one option is to sell it. There are several companies in the business of buying up leases, and they offer a quick, short-term infusion of cash. Typically, a school will get 60 times its last month's rent at once.

"We are purchasing your lease and an easement to the cell site. We give you your one-time up-front cash payment and assume your lease. You are free to do whatever you want with the cash," says Unison Site Management (New York, NY, http://www.unisonsite.com).

Another similar firm is Barkley Tower LLC (http://www.barkleytower.com). They purchase everything from billboard ground leases to telecommunications rooftop space to telecommunication and broadcast towers.

Barkley says most leases that are used to secure the property rights under wireless facilities are essentially short-term lease commitments. That means most leases contain clauses that allow the wireless company to terminate the lease at almost any time, with little or no penalty. There is no other area of real estate that allows a tenant the broad right to terminate in this manner.

These agreements give a third party the right to use the college's land for a specifically stated purpose. A telephone or power company may have an easement from the college to install and maintain the telephone poles on your property. In this case, it would be the operation of a wireless communication site.

The programs might appeal more to office building owners than to large universities, where there could be extensive trade-offs in terms of cellular service for administrators and the like. But for the small college that gets some income from towers and needs a quick cash infusion or protection against that tower rental revenue disappearing, it surely is worth a phone call.

marking and/or lighting may be in accordance with the prior study.

However, if the notice is for a new structure, a physical alteration (height/location) to an existing structure, or an existing structure that did not involve a physical alteration but was not previously studied, FAA says, "The recommended marking and/or lighting shall be in accordance with appropriate chapters of the current AC 70/7460-1, Obstruction Marking and Lighting."

If it is an existing FCC-licensed structure, and the requested marking and/or lighting change is recommended, FAA requires notifying the sponsor to apply to the FCC for permission to make the change.

There is no wiggleroom here. The regulations state, in so many words, that a registrant must "use the following specific language: 'If the structure is subject to the authority of the Federal Communications Commission, a copy of this letter shall be forwarded to them and application should be made to the FCC for permission to change the marking and/or lighting as requested.'" One bit of good news—this specific verbiage is available in the automated letters on the FAA's website.

If the marking and/or lighting change involves high-intensity white obstruction lights on an FCC-licensed structure, the sponsor has to be notified that the FCC requires an environmental assessment.

Again, the language is mandated: "Use the following specific language," FAA says. "FCC licensees are required to file an environmental assessment with the Commission when seeking authorization for the use of the high-intensity flashing white lighting system on structures located in residential neighborhoods, as defined by the applicable zoning law."

Notification of the National Aeronautical Charting Office (NACO) is also required when the change has been accomplished. Once again, there is no room for creative writing. Use the following specific language: "So that aeronautical charts and records can be updated, please notify National Aeronautical Charting Office in writing (with a courtesy copy to the FAA's National Flight Data Center, ATA-110) when the new system is installed and operational. NACO notification should be addressed to: National Aeronautical Charting Office, Aeronautical Information Branch, Room 5601 N/ACC113, 1305 East-West Highway, Silver Spring, Maryland 20910."

If it is determined that marking and/or lighting are not necessary for aviation safety, marking and/or lighting may be accomplished on a voluntary basis. However, marking and/or lighting should not be a condition of the determination. Instead, it shall be recommended that voluntary marking and/or lighting be installed and maintained in accordance with AC 70/7460-1. Got that?

Again, they require the use of specific language as follows: "Based on this evaluation, marking and lighting are not necessary for aviation safety. However, if marking and/or lighting are accomplished on a voluntary basis, we recommend it be installed and maintained in accordance with FAA Advisory Circular 70/7460-1."

By the way, they are not picking on telecommunications towers or colleges. These same regulations cover such diverse structures as suspension bridges and the chimney stacks on power plant.

If the school is just starting to put up a tower, FAA Form 7460-2 (called the Notice of Actual Construction or Alteration, Part 2) has to be submitted. It should be used to report the start and completion of towers. It also has to be filed when a project is abandoned or when an existing structure is dismantled.

In general, it is a good idea to request that sponsors complete and mail Part 1 of FAA Form 7460-2, so it is received at least 10 days before the start of construction. This form must be filled out in many cases. One key metric is the structure's height above ground level (AGL). Any new construction that is more than 200 feet AGL needs a form. So does any tower that might be less than 200 feet AGL but that exceeds obstruction standards. One example would be a tower close to an airport runway or glide path.

### Expiration Dates

Normally all determinations, whether FCC construction-permit–related or not, are assigned an expiration date 18 months from the issued date. These can be extended, revised, or terminated by the issuing office.

Determinations involving existing structures that do not involve a proposed physical alteration do not have an expiration date.

Again, the government is firm on the language used in petitioning information, whether the structure is proposed or existing: "This determination is subject to review if an interested party files a petition on or before (30 days from

issued date). In the event a petition for review is filed, it must contain a full statement of the basis upon which it is made and be submitted in triplicate to the Manager, Airspace and Rules Division, ATA-400, Federal Aviation Administration, Washington, DC 20591. This determination becomes final on (40 days from issued date) unless a petition is timely filed. In which case, this determination will not become final pending disposition of the petition. Interested parties will be notified of the grant of any review."

### Nonflight Considerations

In many cases, adding a new user to an existing tower will create radio or electronic interference. A professional manager of tower space is accustomed to dealing with such problems and will understand the implications of a carrier's request to move an antenna 30 degrees. Unless the school's telecom staff has a wireless EE on call, the implications of such changes can be sticky.

What happens to other parts of many tower deals, like the "free" cellular service often offered to administrators as part of the tower rental package?

"We don't modify the terms of the lease with the carrier," Holmes says. The options are many and include pass-through of the minutes to the school, increased cash payments and termination of the cellular deal, or any other negotiated agreement. Holmes makes it clear that, as a lawyer and businessman, he would prefer the straight cash deal. "It is easier to pass through greenbacks," he says. "But it doesn't make a lot of difference. We're happy to work with a college to make everyone happy."

All of this is enough to make any ACUTA member's eyes spin. Holmes offers one comforting thought: "Normally the tower owner is responsible to do the proper filings, give the correct tower location, and maintain it." If the total height of the building and tower is less than 200 feet, there is no need to mark it.

**Curt Harler** is a contributing editor to the *ACUTA Journal*, a freelance writer, and frequent speaker on technology and other topics.

▼

# The Higher-Ed Spyware Threat

Glenn Taylor

Symantec Corporation

Throughout the past year, dealing with spyware has been rapidly moving up the "to do" list of higher-education CISOs. In addition to potentially stealing private information, spyware bogs down campus networks and reduces student and faculty productivity.

Campus networks present unique challenges. Unlike their corporate counter-parts, university security authorities do not have the relative luxury of limiting network access to a narrow field of specific devices and software. In addition, the large and distributed nature of academic networks makes them difficult to secure because many departments have separate private networks connected to the central campuswide network—which means campuswide policies are harder to enforce.

Meanwhile, software clients who facilitate file trading through networks such as Kazaa are fueling the spyware file. Peer-to-peer networks for bootleg tunes, movies, and software are popular among students. However, restricting file sharing does not block the spyware that is silently dispensed by websites.

In a recent demonstration at Marist College, a staff member used a computer that was known to be free of spyware and adware. Within minutes of visiting websites that are known purveyors of spyware, the machine was laden with hun-dreds of pieces of this pesky software.

### Threat and Risk evolution

Over the past five years, the traditional viral and Trojan-horse threat landscape has evolved. Rapid connectivity and broad use of technology has resulted in an in-creased ability for programs to spread rapidly, automatically export data, and affect systems in a variety of ways.

While fast-spreading worms like MyDoom and Sasser have garnered many of the security-related news headlines, risks from spyware and adware have been steadily increasing. Today, users need to consider not only the threat from viruses, Trojan horses, and worms, but other security soft spots as well. In the future, as reliance on Internet connectivity increases, the impact of not being protected from viruses, Trojan horses, and worms will continue to escalate. Risks from programs such as spyware and adware will continue to require multilevel protection strategies as well as adherence to good security policies.

### Defining Spyware

Programs that are classified as security risks are those that IT departments may wish to detect but that fall outside the sphere of traditional threats like viruses, worms, and Trojan horses. These programs may provide unauthorized access to computer systems; compromise data integrity, privacy, confidentiality, or security; or present some type of disruption or nuisance. They may be introduced into your system by

being unknowingly downloaded from a website or by merely clicking on links or attachments in e-mail messages. They can also be installed after, or as a by-product of, accepting the End User License Agreement (EULA) from another software program.

Spyware and adware programs are closely related, and in some cases, their functions may overlap. In addition, in many cases, they have similar functionality to some viruses and worms. Programs classified as spyware may put universities at risk for identity theft or fraud. These programs may log keystrokes of students and faculty, capture e-mail and instant messaging traffic, or harvest personal information such as passwords and log-in IDs or credit card details. The compromised data is then sent on to one or more people. Depending upon their intention, they may use the information however they wish; for example, accessing and controlling your system remotely or running up charges using stolen credit card information.

Adware, on the other hand, displays advertising that often occurs as, but is not limited to, pop-up windows or bars that appear on the screen and that collect a different sort of personal information: information about the sites users visit, browsing habits, and apparent likes and dislikes.

The risk to the university is considered high if the program attempts to conceal its presence—for example, a program that hides from Task Manager or does not have a user interface. Sending out confidential, sensitive information such as passwords, credit card data, or other personal information is deemed high-risk behavior as well. Likewise, a

measurable impact on a system's stability or performance is classified as high risk; for example, opening multiple windows or spawning processes. Programs that deliberately avoid un-install are often characterized by watchdog processes that reinstall removed programs, duplicate file storage, or store files in unusual or hard-to-find areas. Such functionality is considered to indicate high-risk behavior. Finally, a program is high risk if it possesses functionality that conducts or assists in redirection of users to spoofed websites or non-requested sites.

### Spyware's Prevalence

It's difficult to know how much spyware and adware exist at any given time, as the number is dynamic. However, there are various ways to determine the programs that appear to be most successful or prevalent and to assess whether this prevalence has any impact on your university's network.

The best method of determining prevalence of spyware and adware is to review data specific to spyware and adware, gathered from many credible sources and scientifically analyzed.

Spyware and adware can have a wide range of functionality. For example, at one end of the spyware spectrum, consider the E-Blaster program. This program tracks e-mail, instant messaging usage, and key-strokes. Periodically, it will send e-mail containing the logged information to a

▶

predefined e-mail address. At the other end of the spectrum is the program Spyware.AdvancedKey. This program has similar functionality but must be installed by physically accessing the target computer. Once installed, it creates 16 files, four registry keys, and one service. As with E-Blaster, removal requires the computer to be restarted in safe mode, the files deleted, and the registry keys added by the program removed.

### Reducing Risk

The most effective way to reduce risks from programs classified as security risks is to use a complete security solution that deals with a wide range of threats. In particular, universities and colleges need a solution that categorizes programs according to their functionality and allows them to choose an acceptable risk level. Integrated technologies—antivirus, firewall, and intrusion protection—should work together to provide in-depth defense.

For example, while an antivirus solution works to protect a system against spyware, a firewall allows an organization to create a list of recipients of personal information and to block unwanted advertisements. When a firewall detects that an application is trying to establish an outbound network communication (as a spyware program would to relay information to the outside world), it should automatically close the port and prevent the transmission.

Other issues to consider include the number of spyware definitions supported by a particular solution, the process used for finding new spyware programs, and how the definitions are updated.

To strengthen their defenses, universities should also consider implementing additional security precautions, such as securing encrypted Internet connections, implementing more restrictive Web browser settings, and disabling the acceptance of third-party cookies.

In addition to the use of strong technologies, there are policy measures that can help to reduce risks. For example, make sure that you know and trust the authenticity of any software before you download it and install it. Read the EULAs of software programs to make sure you know what you are getting and tomake sure that you understand and agree with the program's functionality. Examine EULAs carefully to make sure they are in agreement with your security policy. Also, as some spyware is installed using ActiveX controls, consider requiring a prompt for ActiveX to execute within Web browsers.

Stringent rules for downloading and installing software should play a role in establishing this stronghold. Restricting employees from downloading software without the express permission of the IT department is a sure way to maintain defenses. It's imperative to know and trust the authenticity of any software before downloading and installing it. "Just say no!" takes on a whole new meaning when regulating the installation and download of unauthorized computer software.

### Legislation and Standards

The Federal Trade Commission (FTC) warns: "Before using a file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive." Due to the breadth of security threats and risks, it is vital that organizations heed this warning and use security products that can deal not only with spyware and adware, but also with the entire breadth of Internet security threats. Antivirus and firewall products allow users to protect themselves from malicious code such as viruses and Trojans, as well as expanded threats, including spyware and adware.

Recently, legislation to help combat spyware has been introduced worldwide. Spyware legislation was enacted in California and Utah in 2004 and was introduced in at least five other states. At this time, it is impossible to tell how effective the various laws will be in reducing the problem that universities and other organizations face from spyware and adware programs.

### Conclusion

As the spate of recent legislative and FTC activity attests, public intolerance of spyware has reached a new plateau. In the enterprise environment, spyware is rapidly becoming a serious security concern, particularly as most corporate networks allow http traffic, the means by which spyware is propagated.

Spyware is a significant threat, and enterprise users must be vigilant about updating their antivirus software. Security administrators should take extra measures to maintain a strong security posture on client systems. They should also ensure that client system patch levels are up-to-date and that acceptable usage policies are in place and enforced.

Glenn Taylor is Symantec's director of state and local government, hospital, and academic programs. Reach him electronically at glenn_taylor@symantec.com.

▼

# VoIP and Wireless Communications Challenge 911 System

Paul Korzeniowski

The transformation from the public switched telephone network (PSTN) to next-generation (wireless and Internet) services is well underway. Increasingly, students are opting for cell phones rather than landlines. Schools are tinkering with wireless handsets so administrators can send information more easily. Colleges are reducing telecommunications costs by installing voice over IP (VoIP) links. While the new technologies offer many benefits, they also have one limitation: They may not work with 911 services.

Aware of the problem, users, special-interest groups, and the government have been pushing equipment vendors and service providers to support the newer emergency-calling system, dubbed e911. This service not only works with new technologies, but it also provides additional data to emergency responders, such as specific locations inside large buildings, so they are better able to respond to emergencies. While the new service has potential advantages, it also presents significant technical challenges that vendors have only begun to address.

### What's the Problem?

To understand the challenges, one needs to take a close look at how emergency calls are transmitted. They start off in an end-user device, which can now be a wireless or wireline phone, a computer, or personal digital assistant (PDA). The call is then transmitted to a central call-routing system, such as a PBX or voice communications server. Next, the call is handed to a service provider who then delivers it to one of approximately 6,000 911/emergency call centers located throughout the United States. These centers are known as public safety answering points (PSAPs). PSAP personnel then work with local responders to provide emergency services.

The old 911 system worked because the end points were fixed, and the PSTN carried the caller information—basically caller ID data such as name and address—along with the call throughout the transmission. That is not the case with the new telecommunications systems for a few reasons. First, users are no longer stationary, so no one can be sure where a call may originate. Unlike the PSTN, IP networks were not designed to identify callers' locations but instead whether or not they were authorized to access the network.

"IP and cellular networks do not provide visibility to the end user; instead they only 'see' down to the switch or server controlling the call," said Matthias Machowinski, directing analyst, enterprise voice and data at Infonetics Research. This creates problems because in a campus, students and administrators freely travel from one wireless PBX or LAN access point to another. Theoretically, an ambulance could be routed to a campus data center while a 911 caller actually is a mile away in the university's recreation center.

▶

### The FCC Steps In

Vendors and the government have been trying to rectify that problem. Currently, there are lots of workarounds, but no standard way to ensure location data is available with every call. The FCC has emerged as an important force in this discussion, even though its initiatives fall short of being a panacea (see sidebar). In 2000, the government agency started focusing on enhancing wireless networks, so they could support e911 services. That was important because in the United States, wireless users place 50 million (approximately 30 percent of the total) 911 calls each year, and that number has been steadily rising. The FCC embarked on a five-year plan that will be completed in December 2005. Once complete, this phased approach should enable emergency personnel to identify wireless network users' locations within 1,000 feet of where they place their calls.

The cellular industry has been working on different options, and the most popular one aligns cellular and global positioning system (GPS) technology. GPS systems transmit information from remote devices to satellites revolving around the earth. During the past few years, handset

## The FCC Leaves 911 Holes

There can often be a gap between theory and reality, and such discrepancies are evident in regard to e911 services. The FCC has been leading the charge to ensure that these services are ubiquitous. Although the agency has made progress in its quest, there are a few gaping holes—systems not covered by its mandates and funding questions—in its blueprint.

The FCC is charged with regulating interstate and international radio, television, wire, satellite, and cable communications. The group's focus has been on external services, such as those delivered by telecommunications carriers, rather than on internal services, such as those an IT department would provide a university. Consequently, the government agency has outlined regulations that service providers need to adhere to but has stayed away from telling equipment vendors how their products need to perform.

This work has been left to state regulatory boards. "Currently, only 11 states have policies that feature requirements about how vendors' customer premise equipment needs to support e911 services," stated Rick Jones, director of operations issues at National Emergency Number Associa-tion (NENA), an ad hoc organization geared to promote awareness of and develop solutions to problems with 911 calls. As a result, rather than legal recourse, universities have to rely on equipment vendors' voluntary compliance to ensure 911 services are available to their users in most cases.

For the past several years, the U.S. government has been pushing network equipment vendors and service providers to enhance support for their products and services, but has it practiced what it preached? "At the moment, 60 percent of PSAPs are not able to handle e911 calls," noted NENA's Jones.

In order to work with these new services, emergency responders need to upgrade their systems, and the cost of that project has been estimated at approximately $2.5 billion. Aware of the problem, the federal government has said it will supply $1.25 billion in aid during the next five years and expects local governments to match that funding.

Yet, the federal funding is conditional and subject to congressional approval each year. While the money was in the budget at the start of the process for the 2005 fiscal year, that does not mean it will still be there in its final iteration. With items such as the war in Iraq and educational initiatives such as No Child Left Behind in need of funding, the government has been looking for places to trim spending—and e911 services is one of those potential places.

Groups like NENA are pushing the government to shore up e911 holes, but that may not be the most persuasive option. "Unfortunately, the only time the government pays attention to 911 services is when a tragedy takes place," said Neil Strother, an industry analyst with In-Stat/MDR, Inc. In March 2005, a Houston family was unable to place an emergency call during a home intrusion because its VoIP service provider, Vonage America, Inc., did not support e911 calls. Texas lawmakers sued on the basis that the carrier did not notify users of its service limitation, and some see a connection between that case and the FCC's initiative announced in May to have VoIP carriers support e911 services.

While the FCC has made a great deal of progress in advancing the case for e911 services, the government needs to fill in a few holes before these services are ubiquitous. Until that happens, stay safe!

vendors have included GPS capabilities in their products and service providers have signed agreements with firms like Cell-Loc Location Technologies, Inc., and SnapTrack, Inc., which provide GPS tracking services. As a result, when a 911 call is made from a cell phone, the caller's number can be matched to the GPS location key that is sent to the PSAP, providing responders with a geographical reference point for the caller.

While helpful, this is not a foolproof solution. "GPS systems only work within certain ranges," said Bob Egan, president of consulting firm Mobile Competency, Inc. "If a user is inside a building, the system may not be able to see him."

Another issue is that cellular carriers have missed a few of the FCC deadlines: They were originally supposed to complete the work by the end of 2004 but were granted an extension. "I wouldn't be surprised if there were more deployment delays at the end of this year," said Neil Strother, an industry analyst with In-Stat/MDR Inc.

In May 2005, the FCC turned its attention to VoIP networks. Long term, the federal agency wants VoIP service providers to offer services similar to those offered by PSTN service providers, but the agency has not yet outlined its compliance requirements or established a timetable for adoption. It is investigating various technical approaches that may help VoIP service providers meet three broad goals: include e911 as part of their standard offerings, provide callers' location data, and inform their customers of these features.

As of now, VoIP customers must update their location information, and the VoIP service providers deliver them a means of entering that data. "The effectiveness of the VoIP recommendation is suspect since the user has to update the location data," said Sanford Cohen, president of SWN Communications, Inc., a vendor that makes notification software. "A more effective approach would be based on automatic updates generated by the network."

In its wireless and VoIP initiatives, the FCC outlined broad objectives and then left it up to network equipment vendors and service providers to meet them. Vendors and service providers ▶

## Winter Seminars
## Palm Springs, CA
## January 8–11, 2006
## Renaissance Esmeralda Resort

### Track 1. Mobility & Wireless Issues

Phone services and technologies are evolving very quickly. This seminar will offer case studies of innovative campus uses of IP telephony, cell phones, speech recognition, unified messaging, ACD, auto attendant, and other evolving voice technologies. Technology developments, implementation challenges, security and financial implications will be explored as well.

### Track 2. Best Practices in Telecom Management

Threats to telecom and IT services can come from natural causes such as fire or weather as well as from people involved in hacking, spamming, or terrorist activities. This seminar will address a variety of planning, preventive, and responsive approaches that campuses can take to protect both voice and data resources. Specific topics include risk assessment, 911, business continuity, power issues, and network security.

have been moving in a step-by-step fashion to adhere to the objectives.

Hybrid systems represent a simple and basic improvement to 911 systems. When a 911 call is placed, a university's phones can be configured to dial the campus security office, which can not only respond to the emergency but also relay calls to local PSAPs via the PSTN.

### More Challenges Ahead

Even if the vendors comply with the FCC requirements, there still may be challenges for university communications technology managers. "The FCC initiatives do not address wireless enterprise PBXs or VoIP servers, which many universities operate," stated Bruce Mazza, senior solutions manager at Avaya, Inc.

Many vendors have added e911 service modules to their product lines. Such support exists in Cisco's CallManager IP PBX software: Users manually enter phone locations, and that information is uploaded to local PSAP databases. To track IP phone locations, 3Com Corporation relies on its Network Jack 200, a small four-port switch that is installed as a wall jack replacement. The device includes network mapping tools that trace where a firm's IP phones are located and then transmits the information to a database that can be synchronized with local emergency responder teams' information.

To date, many of the improvements have been based on proprietary technology and offer only limited visibility about a caller's location. In most cases, they offer complete visibility only when a campus has one vendor's network equipment—a possibility but not a probability in most

cases. Also since these approaches are based on proprietary technology, they can be expensive and often cannot be easily mixed and matched.

### Setting Standards

The Telecommunications Industry Association (TIA), an ad hoc standards-making consortium, has been trying to make it possible for wireless and VoIP networks to transmit location data in a standard manner. The TIA's Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) standard, which is now in draft form, facilitates information sharing between end points and network infrastructure devices, such as access points. The specification, which was originally designed to enhance network trouble-shooting and configuration issues, defines a way for Ethernet network devices to advertise information about themselves, such as device configuration and device identification, to other nodes in the network. Theoretically, when an LLDP-MED end point enters an area, it would notify the closest access point, and then that information could be relayed to a 911 operator.

There is also a need for a standard way of registering location data in a university's call system and then delivering it to the nearest PSAP. One option is to use GPS location-based services and IP Dynamic Host Configuration Protocol (DHCP) routing to move the information from place to place. Whenever new devices are added to the network, location gateway servers would relay that data between DHCP servers and the carrier's network, and this would allow the automatic updating and delivery of location information to PSAPs.

### Conclusion

To sum it up, it appears that a few years will pass before information is moved from wireless and VoIP end points to PSAPs in a simple, standard way. While the challenges surrounding 911 services are complex, they do not rank high with communications managers: Infonetics found that lack of support for 911 was ninth out of 13 possible items that would prevent an organization from deploying a VoIP system. Perhaps this is an area that IT managers need to be concerned with: There is the possibility that campuses that lack appropriate e911 support could face legal problems if a call made during an emergency doesn't reach its destination.

While e911 services present telecom managers with a lot of short-term challenges, they do feature some long-term benefits. In addition to providing location information, e911 supporters are looking to take advantage of new multimedia capabilities. In the future, callers may have the ability to send video from emergency scenes, say a camera phone sending pictures of a fire, to dispatchers, or responders may be able to send video instruction, say CPR basics, to callers. "Once e911 services are available, a better emergency services system will be in place," concluded Mobile Competency's Egan. "The question now is: How long will the transition to these new services take?"

Paul Korzeniowski is a freelance writer in Sudbury, Massachusetts, who specializes in networking issues. He is also an adjunct faculty member of the Massachusetts College of Pharmacy and Health Services and the University of Phoenix. Reach him at paulkorzen@aol.com.

▼

# Leveling the Playing Field

Alexander Gelfand

Dressed in do-rags, baseball caps, and jeans that are either too loose or too tight, the young men and women piling into the 169th St. subway stop in Jamaica, Queens, could be urban youth in any big city.

Look a little closer, however, and you'll notice some toting unusual accessories: late-model wireless IBM laptops. From their perspective, the computers are standard issue; what's really unusual is that they can't raise a Wi-Fi signal. For these kids, all of whom attend the Queens campus of St. John's University, the subway is one of the few remaining places where they can't go online.

## Getting Ready for Wireless

In 2003, St. John's embarked on a plan to establish comprehensive Wi-Fi coverage across all five of its campuses in New York City and Italy. The private Roman Catholic institution had already overhauled its routers and firewalls as part of a gigabit Ethernet upgrade in the summer of 2002. But the task of implementing a Wi-Fi network was by no means trivial, especially given the complex spatial arrangements—and sheer acreage—involved.

While St. John's Manhattan campus is basically a 10-story office building, and its graduate facility in Rome a compact set of buildings and athletic fields, its remaining locations in Queens, Oakdale, and Staten Island are traditional rolling-lawn campuses. The Jamaica campus alone covers nearly 105 acres.

To address the challenges, the University opted for a phased implementation beginning in September 2003, initially emphasizing coverage of public spaces such as libraries and cafeterias. By January 2004, all academic buildings were completely covered. According to Joseph Tufano, executive director of technology for St. John's, by

March 2005, students were able to acquire a signal in any classroom and in almost all outdoor spaces, with the exception of a few garages and athletic fields.

After sending out a request for proposals and evaluating multiple bids with the help of BearingPoint, a business consulting, systems integration, and managed services firm, the university settled on an 802.11b solution provided by Contemporary Computer Services (CCSI), the same Cisco VAR that had handled the earlier gigabit Ethernet upgrade. Dr. James Benson, CIO and dean of the University libraries, gives CCSI much of the credit for a smooth and successful roll-out. "We have a lot of capable people," says Benson, "but we didn't have every kind of expertise required for this project." CCSI ultimately helped St. John's install over 500 Aironet Access Points running off the latest version of Cisco's Wireless LAN Solution Engine.

## The Academic Computing Initiative

Impressive as it may be, however, the Wi-Fi implementation was only part of a larger academic computing initiative (ACI) that also included an academic Web portal and a mandatory laptop program. Since the fall of 2003, every incoming freshman has received an IBM R-series ThinkPad packing a Centrino chip. Some 3,100 students were issued ThinkPads in the first year alone, along with 400 faculty who opted to trade their desktops for portables. Thanks to the combined features of the ACI, many students can now register for classes, check their grades, and pay their bills anywhere and anytime.

According to Benson, however, university administrators didn't immediately cotton to the

▶

ACI. "The University had considered this kind of thing in the past and rejected it," he says, largely due to concerns over the potential for laptop theft—especially on public transportation. St. John's is predominantly a commuter school; out of approximately 20,000 students, only about 2,800 live on campus.

Proponents of the plan argued that laptop safety had improved in recent years as laptops had become common commodities and were therefore at lower risk of being stolen. They also contended that students could be taught to protect themselves against theft. Toward that end, an antitheft program called "Operation Laptop" was bundled into the initiative. According to Jody Fisher, director of media relations for St. John's, every student laptop is etched with a unique ID number that is recorded both by the NYPD and by the University's own public safety office. "In the event of a theft or loss, only the person attached to that unique ID number can pick up a recovered laptop," Fisher explained. In addition, NYPD officers come to campus "to instruct students on laptop safety (don't leave it unattended, that kind of thing)." The program appears to be working: Thefts are rare, and the recovery rate for lost or stolen machines is high. Fisher notes that one laptop was recovered as far afield as Ohio.

As was the case with the Wi-Fi solution, the laptop component of the ACI was handled through a competitive bidding process. The University ultimately went with IBM because of the company's prior experience with mandatory laptop programs at Seton Hall and Wake Forest universities. In addition, administrators were impressed with the ThinkPad R-series' long battery life, along with its ability to sense wired or wireless connections and to switch between them without rebooting—all important factors because of the commuter issue. "We

wanted a machine that students could use at Starbucks and McDonald's," says Benson.

### Cost Factors

Overall, the ACI was meant to provide uniform accessibility on a common platform, to "level the playing field," as St. John's officials say, by creating an environment where computing would become second nature to all students, regardless of their economic circumstances. The economic aspect was especially important for St. John's. The University was founded in 1870 by the Vincentian Community, a Catholic order that ministers to the poor and marginalized. As an institution, the university is committed to educating the underserved.

As a result, St. John's sought to implement the ACI without unduly burdening students financially. Initial startup costs for the Wi-Fi network and laptop distribution program came in at approximately $7 million. But according to Fisher, incoming freshmen paid only $600 more than returning students in 2003, with the University itself picking up the rest of the tab. In 2004, tuition went up by 7.5 percent for both new and returning students. "We made a conscious decision to make it part of tuition so it would be covered by financial aid," says Tufano. That coverage is a crucial economic factor at St. John's, where 80 percent of students already receive some form of assistance. "A laptop is simply out of the question as an out-of-pocket expense for most of them," says Fisher.

Ongoing costs, such as software and insurance, have proven to be "very reasonable," says Tufano. And thanks to strenuous cost containment, some staff retrenchment, and the elimination of a few computer labs, St. John's has been able to manage the program at less than 2 percent budget growth per year. The ACI appears to be an even better value when one considers that faculty may eventually substitute virtual classroom

hours for real ones. "As teaching is transformed, the number of classroom teaching contract hours will decline, and the need for building space will also decline," predicts Benson. Over time, that could lead to tens of millions of dollars in savings, although, as Tufano admits, "that's not going to happen in a year."

### Supporting the Program

Getting the ACI rolling required more than just installing wireless routers and handing out ThinkPads. St. John's also had to expand its technical support and training programs. The University qualified its own technical staff to act as IBM repair technicians and assigned support personnel to each academic building. It also created what Tufano calls the "laptop shop," a full-service support system that handles everything from accidental damage to theft. The University plans to incorporate an IT orientation component into Discover NY, a core course that all students must take within their first two semesters. And faculty receive stipends for completing the University's Portable Professor workshops ($250 for the first two and an additional $250 for a third), where they learn to do everything from using e-mail to posting syllabi online.

Tufano believes that the greatest challenges involved in implementing the ACI weren't technical but organizational. And, as he is quick to point out, the initiative itself was always about more than just hotspots and laptops. "It's not a technology project," he says. "It's a *University* project. We didn't lead with the technology. We led with the question, 'How can we serve our students and faculty?'"

**Alexander Gelfand is a freelance writer as well as an occasional assistant professor at St. John's and a former IT professional at a leading online education company. Reach him at mail@alexandergelfand.com.**

▼

# The University of Texas at Austin



*At ACUTA's 34th Annual Conference, the University of Texas at Austin was recognized for its TXShop with the Institutional Excellence in Communications Technology Award. We salute the University with this description of their project, taken from materials they submitted in application for the award.*

TXShop is the online shopping mall of the University of Texas at Austin that allows any University department to open a store from which they sell products and services or offer event registrations to anyone with Internet access. The University's information technology services–enterprise information services (ITS-EIS) maintains the TXShop application, which is part of the secure administrative network.

TXShop began as a response to a specific request by one department, but it quickly evolved to become the more generalized, customizable system it is today. ITS-EIS was first contacted by continuing and extended education (CEE) in fall 1999 about creating a shopping system to sell seminars and class registrations. TXShop version 1.0 was undertaken specifically for CEE, but when the division of housing and food services (DHFS) expressed a similar interest, ITS-EIS recognized the potential for developing a centralized, University-wide, shopping cart application, thus making version 1.0 obsolete before it was ever released.

Version 2.0 was released in April 2002 when Hug 'Em Horns, the DHFS store, officially opened for business offering gift baskets, balloons, and Bevo Bucks to students living in campus housing. ITS-EIS team members maintained the Web and server elements driving TXShop, while department store administrators were responsible for the content and maintenance of their stores.

TXShop is now in version 3.0. Its unique flexibility accommodates an enormous range of departmental stores, and additional clients have continued to join. Store administrators benefit from a robust administrative suite and on-site technical support. Departments can specify member discounts, shipping rates, and special product information, and each online store is customized by its administrators to give a distinctive appearance to the merchandise they offer.

Another unique quality is the ability of departmental programmers to use application program interfaces (APIs) to incorporate their own business processes into TXShop operations. For instance, software distribution and sales uses an API to determine availability and price based on the customer's relationship (student, staff, or other) to the University.

The customers of TXShop 3.0 include University staff, alumni, and even the public at large. The Bureau of Economic Geology sells topographical maps nationwide; Software Distribution and Sales provides downloadable software to faculty, staff, and students; the Office of Development has sold conference registrations to the 2005 Big XII Development Conference; the Texas Memorial Museum has opened a virtual gift shop. In this era of diminishing funding for higher education, TXShop provides an opportunity for departments to market and sell their products and services to a wider audience than previously possible.

▶

Currently 30 stores are set up in TXShop, and two new stores are in the setup process. TXShop sales for 2004 were up 500 percent over 2003. The Charles A. Dana Center sold more than $180,000 in educational materials to K-12 teachers, and the School of Music sold more than $285,000 of summer band camp registrations.

TXShop offers more, however, than just the opportunity to sell. Work is ongoing to allow the application to accept donations in accordance with University regulations. The University of Texas Libraries is planning to open a store to fund books, and the Blanton Museum of Art is planning to sell tax-deductible memberships, part of which is considered a donation.

### Planning, Leadership, and Management Support

Making TXShop a reality required a concerted cross-departmental effort undertaken both by the TXShop development team and ITS-EIS management.

After ITS-EIS management committed in 2001 to reinventing the initial application as a generic online shopping mall serving all departments, the team began to reach out to the application's potential clientele. The four-FTE development team set up a client working group open to any department on campus interested in selling products or services online. This working group crystallized into a core set of clients comprising the Bureau of Economic Geology, the Charles A. Dana Center, the Texas Memorial Museum, and DHFS. The leader among these client-advisors was DHFS whose "Hug 'Em Horns" store was the first to open in TXShop. TXShop development team leader Angela Svoboda and DHFS assistant director Sheila Ochner worked together to ensure the success of Hug 'Em Horns. The store did indeed thrive, and it demonstrated the flexibility of the TXShop model to other departments.

While the development team worked with future store administrators to identify desired functionality, management in ITS-EIS, the Office of Accounting, and the office of the vice president and chief financial officer cooperated to ensure that implementation was in line with the University's mission, regulations, and procedures. From a policy perspective, the office of accounting had to embrace the concept of ITS-EIS administering a shopping cart application that plugged directly into its own centralized receivables machinery. This would mean more work for many financial personnel, including (1) reviewing items for sale to make sure that they adhered to the University's mission, (2) creating financial accounting codes for each department coming into the system, (3) processing refunds for credit card orders, and (4) devoting technical resources to helping the TXShop development team integrate its code with accounting modules. The Office of Accounting, therefore, made a significant investment in an application that it neither initiated nor owned.

At a university as large and decentralized as UT-Austin, such departmental partnerships often encounter ingrained resistance. The success of the TXShop partnership was due in large part to the diligent negotiations of Randy Ebeling, associate vice president for information technology, and Fred Friedrich, director of accounting. These departmental leaders recognized that TXShop would advance the University's mission to be a "university of the first class," enriching the lives of all Texans by empowering departments to conduct business more efficiently and to offer products and services beyond campus.

Growth of TXShop from its release has been steady. In January 2003, the system had five stores; in February 2004, after the Version 3.0 system upgrade, 12 stores were online in TXShop; today 30 stores have been created. (Along the way, two have

closed up shop.) Each store represents an ongoing relationship between the departmental store administrators and the TXShop development team. The increasing number of stores has brought increasing complexity. To guide TXShop into maturity and prioritize requests for new functionality, a six-member executive oversight committee (EOC) was created in late 2004. Its membership of two ITS directors, two departmental store administrators, and one accounting manager reflects the cross-departmental nature of the application.

### Promotion of Technology and Maturity of Effort

UT-Austin is on the cutting edge of communications technology. Its Internet bandwidth has been boosted from 90 Mbps to 180 Mbps, and it recently formed a partnership with the Texas department of information resources (DIR) to further boost bandwidth resources for organizations across the state that connect via THEnet. In partnership with the University, DIR has purchased a higher speed circuit providing 622 Mbps of bandwidth. This bandwidth is divided up among THEnet subscribers based on monthly subscription rates and service level agreements. The University is a THEnet customer and has benefited greatly from the larger allocation of bandwidth.

Security is a key element in the University's Web systems and is especially important to an application such as TXShop. In order for customers to use TXShop, which is hosted on the secure UT direct server, they must have Web browsers that support SSL encryption. In addition to the encryption of transactions, TXShop makes use of Verisign's secure credit card processing technology.

Another element of security is authenticating the user. The University's UT EID (electronic identity) system was implemented in 1995 to support the issuance of physical ID cards. At that time, a

database was created to house biographical information for each person with a UT EID. As the system evolved and the University started providing Web-based services to users, the UT EID grew in importance. Almost anyone who has significant dealings with the University—students, prospective students, employees, job applicants, business entities, donors—has a UT EID. Stores in TXShop have the option to use the authentication capability of the UT EID, and some employ it to determine if the customer is eligible to buy its products; other stores either do not require UT EIDs at all or offer the shopper the ability to obtain a guest UT EID during the checkout process.

With its centralized payment processing technology and ability to be customized to fit any department's e-commerce needs, TXShop is the state-of-the-art. IT-EIS is aware of no other institution offering a similar integrated shopping mall package.

### Quality, Performance, and Productivity Measurements

During the initial planning of TXShop, the development team recognized that the customer interface was paramount to the project's success. The TXShop homepage may be the customer's first interaction with the University, and a consistent and pleasant experience was viewed as a crucial element of design. This focus on the look and feel of TXShop has increased quality by providing a consistent customer experience across all TXShop stores.

Within TXShop's consistent interface, however, are many options allowing the administrator to configure the individual store. For example, an administrator may select from several different color themes, spotlight items, use unique graphics, and attach a different image to each item or service within the store. He or she can collect input from the customer at several points during the shopping process; i.e., a store might ask customers what information they would like printed on an event badge or request the size and color of a t-shirt that is being ordered.

TXShop allows even more store flexibility through the use of APIs that allow external departmental control of many processes within the system. Using these APIs, the administrator can control what items a customer may purchase based on specific criteria. Other examples of API usage include using an external database to control inventory levels, customizing payment methods, or computing special shipping charges. APIs have allowed stores in TXShop to perform processing that TXShop's core functionality could not provide. It is an outstanding example of combining decentralized processing into a centralized system.

Significant management oversight was recognized as necessary for full quality control of all products and services offered through TXShop. These controls ensured that the application would meet the well-defined standards of the University. All products and services must be approved by the vice president and chief financial officer.

Adherence to University regulations is also achieved through a TXShop rights and responsibilities document developed by the EOC. This document outlines what is required and expected of store administrators and the TXShop development team.

The rapid growth and acceptance of TXShop by the University community is evidence of the robust performance of the application. In 2002 the application processed more than $14,000 in revenue; by 2003 that figure exceeded $100,000; and in 2004 stores collected more than $607,000 in revenue. TXShop rocketed past the $1 million mark in sales in May, 2005, doing more than $147,000 in May alone. This growth could never have been accomplished without the superb performance of the application in meeting customer expectations.

TXShop performance has been additionally enhanced by the optional feature for a customer to complete a shopper profile to be permanently retained on file. When a customer with a profile returns to TXShop for a future purchase, he or she will find billing and shipping information pre-populated into all order-processing functions, providing convenience and time savings.

Prior to TXShop, many departmental attempts to provide products and services were being met by time-intensive manual systems, while some were not being attempted at all due to manpower and time constraints.

For example, event registration has become the fastest-growing type of store within TXShop. Some departments may have only one event a year, while others may spread several events throughout the calendar year. Before TXShop, each department had to develop its own database management system to manage event information. If the department wanted to accept credit card payment, it had to obtain its own credit card machine and manually enter all financial data into the University accounting system. With TXShop's ease of use, a nontechnical store administrator can set up an event and begin taking registrations within a matter of a few hours. Credit card processing is centrally controlled and automatically integrated into the University accounting system. Event setup can be retained to be used again or modified to fit a future event.

TXShop's flexibility has been highlighted with a recent innovation by DHFS, which maintains several dormitory and food facilities spread out across campus. DHFS has creatively decided to use TXShop to control and distribute the consumables used across their operation. Authorized employees can go online and request that supplies be delivered where needed by entering a no-cost order in TXShop. TXShop's creators never envisioned that a

▶

department would use the application exclusively for inventory control, and yet the system is proving very suitable for that function.

## Cost, Benefit, and Risk Analysis

The development of TXShop was a speculative venture. ITS-EIS management envisioned a campuswide online shopping mall and realized that this vision aligned well with the long-range goals of ITS-EIS to provide University IT infrastructure. In terms of initial funding, management decided to support development entirely from the budget of the central ITS group. Although ITS-EIS would see limited, if any, economic benefit from the product, enabling departments to offer products and services more efficiently fulfilled its mission and justified the cost.

During TXShop's initial development leading to the release of version 2.0 in April 2002, two to four FTEs worked on the project at any given time. In the fall of 2003, a four-month major enhancement effort was undertaken by six FTEs culminating in version 3.0. This project provided additional functionality and enhancements that led to reduced maintenance requirements. The application is currently supported by one or two FTEs for maintenance and client-relation purposes.

ITS-EIS has never charged fees for TXShop services, but as the application has grown and more stores have opened, this funding model has become harder to sustain. In late 2004, the TXShop EOC began doing true cost-benefit analyses in order to develop a funding model that will allow TXShop to maintain its high standard of service. No final decisions have been made, but stores may soon be asked to pay an initial setup fee and to fund the development of special features they request.

## Customer Satisfaction and Results

TXShop has seen a consistently expanding user base and a correspond-ing increase in client involvement. To accommodate this growth, new mechanisms for overseeing the application have had to be developed.

When TXShop began as a joint project between ITS-EIS and CEE, the development team relied heavily on its single client in the planning and implementation of the endeavor. However, CEE's influence was marginal compared to that of the working group of clients that came together in 2002. These founding clients had heard about TXShop's development largely by word of mouth. They included the Bureau of Economic Geology, the Charles A. Dana Center, the Texas Memorial Museum, and, most importantly, DHFS. The experiences of these pioneering departments led to a suite of enhancements that was released in January 2003 under the name TXShop 2.0.

User reaction to TXShop 2.0 was very positive, leading to an increase in the number of stores, and with it, an increase in the number of enhancement requests. The departments that had begun to use TXShop saw its potential for handling more and more of their business needs. Requests came in, for example, to increase shipping options, give customers the ability to make purchases without having to get a UT EID (especially important to departments wanting to sell to the general public), and provide administrators with the ability to upload and download data. Recognizing the growing backlog of requests, in summer 2003 ITS-EIS management committed to a four-month development project culminating in version 3.0 of TXShop.

The TXShop 3.0 versioning effort reflected the application's growing client base. The development team employed a designated product manager responsible for developing a comprehensive communications plan, holding town hall forums for current and prospective departments, and more fully marketing the application campuswide. The project succeeded at delivering additional core functionality that existing clients desired, and upon completion, TXShop 3.0 was spot-lighted on the University's home page.

Today, more than a year after TXShop 3.0's release, the shifting balance between application maintenance and client communications can be seen in the fact that ITS-EIS dedicates one FTE as a liaison between itself, accounting, and the ever-growing community of departmental store administrators. This person handles all client e-mails, assists new stores in the setup process, holds administrative training sessions, and generally addresses all nontechnical TXShop issues. Clearly, as the number of TXShop clients has increased, the communications strategy has evolved to meet the demand: from working groups to a version product manager to today's designated TXShop communications specialist.

Any application as far-reaching and ambitious as TXShop will encounter unanticipated challenges. The very notion of creating a centralized online store for all University departments is fraught with complexity since no two departments sell the same thing in the same way. It has been rewarding to see that most of the unanticipated challenges have come from departments that have embraced the core functionality of TXShop and requested one or two more features to facilitate business in their particular stores. Success has bred new requests. TXShop is thus constantly evolving, striving always to give departments more latitude beyond the core processes to which all stores must adhere. To this day, TXShop continues to listen to its client departments and find ways to empower them to conduct business.

Tracy Brown is assistant director of ITS – Enterprise Information Services. She can be reached at t.brown@its.utexas.edu. Material for this award was submitted by Tracy Brown, Tim Chamberlain, Bennett Donovan, and Larry Wilburn. UT Austin's primary ACUTA representative is George Denbow. George can be reached at g.denbow@austin.utexas.edu.

▼

# Bill D. Morris Award

The Bill D. Morris Award, one of ACUTA's two prestigious individual awards, is presented at the annual banquet to the member deemed by the president to best exemplify the dedication, vision, professionalism, and leadership brought to ACUTA by the late Bill Morris. Morris, from the University of Central Florida, served the association as president in 1988–89.

At the 34th Annual Conference in Kissimmee, President Tamara Closs named the winner of the award for 2004–05: Jeanne Jansenius from the University of the South in Sewanee, Tennessee.

Jansenius joined ACUTA in 1995 and in the same year began serving as a member of the Program Committee, which she chaired from 1997–99. In 1999 she was elected to the board, serving as director-at-large before becoming president in 2002–03. Along the way, she coordinated efforts with MiCTA to form a wireless working group. Having completed five years of board service, she continues to serve ACUTA as a member of both the Journal Editorial Board and the Communities of Interest Task Force .

In addition to her ACUTA accomplishments, she chairs the Network Infrastructure Team for her campus and has served as president of the Nortel SL1 User Group for the state of Tennessee.

Jeanne is respected by many not just for her professional success, but also as a warm and caring friend. Genuine and unpretentious, she is always an interested  listener, generous with her time and her talents.

She is recognized as a tireless worker on the campus of the University of the South, having learned about communications technology after coming from a business background. Projects undertaken on her small campus frequently impress even those whose budgets and resources are many times what hers may be.

Truly a lifelong learner, Jeanne Jansenius sets a standard for excellence to which everyone should aspire. She does, unquestionably, personify the qualities that this award represents.

▼

*At the 34th Annual Conference, ACUTA President Tamara Closs named former ACUTA President Jeanne Jansenius winner of this year's  Bill D. Morris Award.*

# ACUTA Legislative and Regulatory Affairs Committee Works for You

Dave Ostrom

Washington State University

ACUTA's Legislative/Regulatory Affairs Committee has begun the new year with a great start. On August 10, 2005, Jeri Semer and I met with four staff members from the FCC's Wireline Competition Bureau, Telecommunications Access Policy Division to provide information regarding the potential impact of the numbers-based contribution methodology for the universal service fund (USF). We had a great discussion with the FCC staff members reacting to the impact (using Washington State University figures) and asking for further information. This meeting, along with ACUTA being represented on the FCC Consumer Advisory Council (see page 15), will help to establish ACUTA with the FCC as an organization that represents higher education and is a source for information regarding potential regulatory decisions.

ACUTA members can support these efforts by helping the committee and the ACUTA professional staff to collect information as it is needed to support filings with the FCC or to assess the impact of potential rulings. On several occasions we have asked for such information through Web-based surveys. A broader response would provide data that more accurately reflects the impact on ACUTA members and would help us make a more compelling case. At times our requests for information may require work on your part, and we really appreciate the time and effort you spend responding. I've also heard that some questions or intent may be confusing, and I urge you to call the ACUTA office should you need clarification. If necessary, they can pass the question on to the committee for a response.

### Legislative/Regulatory Affairs Committee

| Name | Affiliation | Email |
|---|---|---|
| David W. Ostrom, Chair | Washington State University | ostrom@wsu.edu |
| Angel N. Dronsfield, Member | Duke University | angel.dronsfield@duke.edu |
| Christopher B. Peabody, Member | L. Robert Kimball and Associates | chrispeabody@lrkimball.com |
| Doris A. Stock, Member | Virginia Tech | stockd@vt.edu |
| Ed Quinn, Member | Ohio State University | quinn.2@osu.edu |
| Gregory A. Stahl, Member | St. Lawrence University | greg@stlawu.edu |
| Lorenza Nunez, Member | Texas A&M University | lnunez@tamu.edu |
| Walter L. Czerniak, Member | Northern Illinois University | wczerniak@niu.edu |
| Whitney L. Johnson, Member | Retired, Northern Michigan Univ. | wjohnson@nmu.edu |
| Patricia H. Todus, Ex-Officio | Northwestern University | p-todus@northwestern.edu |
| Phillip Beidelman, Board Liaison | WTC | pbeidelman@wtc-inc.net |
| Jeri A. Semer, CAE, Staff Liaison | ACUTA Executive Director | jsemer@acuta.org |

### In the Months Ahead

The Leg/Reg Committee's goals for the next several months include further work on the USF contribution methodology due to its potential impact on ACUTA members and the FCC's desire to finish the development of a model by the end of December, 2005. We will also be watching what action the FCC takes on the Communications Assistance for Law Enforcement Act (CALEA). Part of the law directs the FCC to identify telecommunications services that are subject to the requirements of CALEA which are not specifically detailed in the law. ACUTA participated earlier in a shared filing with EDUCAUSE and others that was sent to the Department of Justice (see http://www.acuta.org/?1264.) The filing made the case for an exemption for higher

education from the provisions of the act. We will have another chance for input when the FCC issues a Notice of Proposed Rulemaking (NPRM) this fall.

While it is unclear as to whether or not there will be substantive action this fall, we are closely watching the news concerning the rewrite of the 1996 Telecommunications Act. Activity is increasing, although some say that it may take years for a bill to be fully developed. The Leg/Reg Committee hopes to find a way to provide input as the new law is developed so that significant negative impacts on ACUTA members can be avoided.

Another important goal of the Leg/Reg Committee is to fully participate in advancing ACUTA's recently adopted strategic goals. Our work with the FCC supports the goals as does the development of white papers regarding legislative and regulatory topics. Work on the white papers in cooperation with the Publications Committee will be a key objective for the next several months as it is hoped that these white papers on topics such as E911, USF, and Inter-Carrier Compensation will be a valuable resource to all ACUTA members.

In summary, the committee is engaged in important work on behalf of all ACUTA members. Participation on the committee can provide enrichment to your job as well as education that can help the institution you represent in addition to all of higher education. I would like to encourage participation on the committee and ask that you contact the ACUTA office if you are interested. Talk to any current member about the rewards of serving on this committee.

**Dave Ostrom is chair of ACUTA's Legislative and Regulatory Affairs Committee. Reach him at ostrom@wsu.edu.**

▼

# 35th Annual Conference

## San Diego, CA

## July 23–27, 2006

## Manchester Grand Hyatt

# Advertisers' Index

★ Indicates ACUTA Corporate Affiliate

By advertising in the *ACUTA Journal,* these companies are not only promoting products and services relevant to telecommunications in higher education, they are also supporting our association. As you have opportunity, we encourage you to mention to these companies that you saw their ad in our journal.

For information about advertising in the *ACUTA Journal,* contact
Amy Burton, Manager of Corporate Relations and Marketing, at 859/278-3338 or aburton@acuta.org.

model (suppliers, input, processing, output, customers)—with storage added—provides a useful checklist. Ask questions such as "Who creates or supplies data? Who uses or handles data?" For input, consider both manual and automated methods. Output includes reports, screen look-ups, downloads, e-mails, and auto-mated interfaces, as well as documents where information is stored and on what media.

Also look at your institution's safeguards for information. In teaching a graduate course on risk assessment and information security manage-ment, I assign students projects that force them to look at safeguards in multiple ways. For example, they use the NIST (National Institute for Standards and Technology) model of managerial, operational, and technical controls. Another lens for looking at safeguards is that of confidentiality, integrity, and availability. The third approach is based on prevention, detection, and response/recovery of incidents. Table 1 provides an example of each.

Your campus incident response plan will need to be broadened for the Identity Theft Protection Act to include steps for notifying people whose records may have been exposed without authorization. Public relations staff for your institution will need to be deeply involved, and you should plan to use multiple communications channels for keeping victims informed. For example, draft sample notification letters and create a shell of a notifica-tion Web page. And talk to people affected; a survey showed that telephone contact made the victims feel better about the situation.

| Table 1. Types of Safeguards and Examples | |
|---|---|
| Managerial | Establish security requirements for systems, whether developed in-house or purchased |
| Operational | Procedures for disposal of storage media and systems |
| Technical | Encryption |
| Confidentiality | Access controls |
| Integrity | Monitor systems for root kits |
| Availability | Store backups off-site |
| Prevention | Have physical and logical locks |
| Detection | Review audit trails and logs |
| Response/Recovery | Automatically shut off an account after three failed log-in attempts |

Consider using a call center with both inbound and outbound capabilities, and design it with all the usual features: toll-free number, lines for volume, mailboxes, and so on. The call center's software should support, for example, scripted answers to calls and tracking of communication (by both phone and mail). Also, have established contacts with both law enforcement groups and the credit bureaus available to connect people who feel they are victims of identity theft. Finally, as with any incident response plan, provide regular training and testing.

Marjorie Windelberg, Ph.D., is the principal consultant at Windelberg Consulting, LLC. An active contributor to ACUTA publications and frequent presenter at ACUTA events, she can be reached at Marjorie@windelbergconsulting.com.

▼

## Here's My Advice



**Marjorie Windelberg, Ph.D.**
**Windelberg Consulting, LLC**

# How's Your Incident Response Plan?

Data losses and exposures have been regular headlines during 2005, with several higher-education institutions from George Mason University to the University of California at Berkeley sharing the unwelcome spotlight with businesses like ChoicePoint and LexisNexis.

The uproar prompted congressional action. In late July 2005, the U.S. Senate passed the Identity Theft Protection Act, which imposes requirements on educational institutions, among others. Similar to the California law familiarly known as SB 1386 (its formal designation is Civil Code 1798.29), the act requires disclosure of security breaches within 45 days if the breach involves a "reasonable risk" of identity theft. The proposed act also requires organizations to have formal programs for securing sensitive information and empowers the Federal Trade Commission (FTC) to mandate both physical and technological safeguards.

If passed by the full Congress, this new regulation will join other privacy and information security laws such FERPA, GLBA, and HIPAA that impose obligations on colleges and universities and can entail penalties if violations are uncovered. The new act should be seen as an opportunity to review your institution's privacy and security program or, if you haven't completed one yet, to get working on it.

Start with a review of policies. Do policies address personally identifiable information, including where and how such information may be stored, reported, or shared? Is anyone using social security number as an ID or record key? Don't forget faculty and staff: Require them to undergo awareness training, to safeguard information, and to report suspected breaches to proper authorities. For certain employees, it may be appropriate to have them sign rules of behavior that incorporate confidentiality requirements.

Determine if your information asset inventory is up-to-date and accurate, focusing on data that are critical and sensitive (intellectual property, in addition to personally identifiable information). The SIPOC

## How to Champion Privacy

1. Educate yourself and others on current and anticipated privacy regulations.
2. Work with senior management and natural allies (such as human resources, auditors, and legal counsel) to promote and instill a culture of privacy.
3. Develop, maintain, and enforce privacy policies and a written program for securing sensitive information and responding to incidents.
4. Assess risks and follow through with risk-mitigation plans. Then do it again and again, because the threats, vulnerabilities, and regulations keep changing.
5. Be vigilant about safeguarding data through awareness campaigns and automated controls.

$$\left\{\left[(DATA\ Services)^2 + \begin{matrix}BAND\ WIDTH \\ USER\ POP.\end{matrix}\right.\right.$$

$$+ \left[\frac{(WLAN) + (VOIP) + (VID)}{NETWORK\ \ MGMT}\right]\right\}$$

$$+\ \begin{matrix}UNIFIED \\ MESSAGING\end{matrix}$$

$$=\ TOTAL\ SOLUTION$$

# When You Add It All Together, The Answer is NEC

Let NEC formulate the ideal communications solution for your campus environment.

Whether deploying IP Communications across a campus or providing comprehensive services that enhance your network performance, NEC helps you balance the equation between business requirements and technology solutions.

Empowered by Innovation     **NEC**