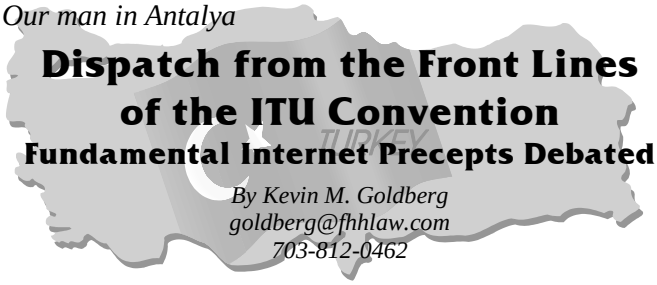
FLETCHER, HEALD & HILDRETH, P.L.C.

FHH Telecom Law

Current Issues in Telecommunications Law and Regulation January 2007

Our man in Antalya



Dispatch from the Front Lines of the ITU Convention

Fundamental Internet Precepts Debated

By Kevin M. Goldberg
goldberg@fhhlaw.com
703-812-0462

Even for those who possess a strong working knowledge of telecommunications law, experiencing an international conference such as the International Telecommunications Union's (ITU) Plenipotentiary Conference in Antalya, Turkey can best be described as "an entirely different world." The conference is held every four years in order to transact the overall business of the ITU and to add, delete and update the organization's governing documents and implementing regulations. Though I have worked on international press freedom and related telecommunications issues for several years, attending an official conference requires knowledge of more than just the underlying law and policy. One must also navigate sensitive international political and diplomatic issues which constantly obstruct seemingly straightforward solutions. I often contemplated this fact as the most obvious answers were dragged through days (and nights) of negotiation until compromises were reached that would accommodate everybody.

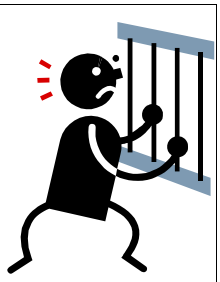
This year's ITU Plenipotentiary Conference was a somewhat new experience even for grizzled veterans of the international telecommunications arena due to an intense focus on matters related to the Internet. In addition to the usual ITU committees dealing with structure, budget and other organizational tasks, the Plenipotentiary Conference featured a special "working group" related to implementation of policies agreed to during the two-phase World Summit on Information Society (WSIS). In particular, I became involved in negotiations over two resolutions which would affect online content, extending the potential reach of the ITU beyond telecommunications and into areas affecting television, radio and even news-

(Continued on page 10)

Users freed to move around

Government Unlocks Cells

By Patrick A. Murck
murck@fhhlaw.com
703-812-0476



Just after Thanksgiving, the U.S. Copyright Office gave consumers something extra to be thankful about by allowing them to lawfully "unlock" their cellphones for use on any service provider's compatible network. Now, you may wonder why the Copyright Office of the Library of Congress is regulating consumer's ability to keep their cellphones when they switch providers. Well, the answer is simple (in that Washington lawyer kind of way) – Congress gave the Copyright Office authority in the Digital Millennium Copyright Act (DMCA) to exempt certain classes of work from the anti-circumvention language in §1201 of the DMCA.

This section of the DMCA was designed to enhance Digital Rights Management (DRM) software that protects digitized, copyrighted works from piracy. However, Congress recognized that creating statutory penalties for circumventing all DRM schemes, even when they are protecting things not subject to regular copyright protection, would have been overbroad. Thus they created a release valve of sorts, by empowering the Copyright Office to create exempt classes of works that don't receive anti-circumvention protection under §1201 of the DMCA. The statute requires the Copyright Office to hold a rulemaking proceeding every three years to determine which classes of works should be exempted from §1201 protection.

In this latest rulemaking one of the exempted classes of works was created because of complaints about cellphone service providers equipping the phones they sold with "software locks" preventing access to the phones' "bootloader" program. Denying consumers access to this program had the effect of restricting the networks the

(Continued on page 8)

Another good reason to avoid litigation

New Court Rules Address Preservation, Disclosure of Electronic Files In Litigation

By Patrick A. Murck
murck@fhhlaw.com
703-812-0476

After seven years and one major revision, the latest amendments to the Federal Rules for Civil Procedure became effective on the first of December. So what, you ask? As it turns out, the new rules could affect you if you ever wind up involved in litigation in a federal court.

Included in the revisions are new rules for dealing with electronically stored information during discovery, so-called "e-discovery." Of particular concern here is the fact that the new e-discovery rules set out a roadmap for how electronically stored information can be used during the "discovery" portion of litigation.

As any of you who have had the misfortune to find yourselves in litigation probably know, one of the most burdensome aspects of that process involves "discovery". Discovery is the pre-trial phase of the proceeding during which each side has the right to ask the other side to cough up all information, documents, witnesses, etc. that might be relevant to the issues to be litigated. Contrary to the mythical trial process depicted on *Perry Mason* and innumerable other TV series, the real-world trial process is designed to prevent any sudden surprises popping up during the trial. Discovery is the main device through which that goal is accomplished. The idea is that each side of the litigation should know what cards the other side is holding before the trial starts, so that the issues can be narrowed and the trial process streamlined as much as possible.

As a result, when litigation is commenced, one of the first major chores is answering the other side's discovery requests, which normally include requests for all relevant documents of any kind that a party (including the party's employees, agents, etc., etc.) may have anywhere in their files.

Historically the search for responsive documents involved a tedious review of all paper files. But with the advent of electronic data storage, courts have had to grapple with a variety of new issues. For example, we all know (from the Enron episode, and before that, the Ollie North/Fawn Hall episode) that shredding documents can get you into trouble. But what about erasing electronic files (for example, pesky emails) – isn't that pretty much the same type of conduct?

The newly revised federal rules reflect an effort to begin to address such questions. While this is an area which is still in the process of evolving, here are some considerations which businesses should bear in mind, even if they are not currently involved in any litigation.

Businesses should have a general policy relating to electronic document retention and storage. A key provision of the new e-discovery rules is the limited "safe harbor" provision in Rule 37(f) that shields a litigant from sanctions for overwriting electronically stored information. The rule acknowl-

(Continued on page 13)

Fletcher, Heald & Hildreth
A Professional Limited Liability Company

1300 N. 17th Street - 11th Floor
Arlington, Virginia 22209
***Tel*: (703) 812-0400**
***Fax*: (703) 812-0486**
***E-Mail*: editor@fhhlaw.com**
***Web Site*: fhhlaw.com**

Editor
Donald J. Evans

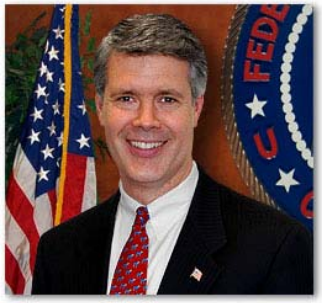
Design
Harry F. Cole

Contributing Writers
Jeffrey J. Gee, Kevin M. Goldberg, Frank R. Jazzo, Mitchell Lazarus, Patrick Murck, Lee G. Petro and Ron Whitworth

New Commissioner just says no

McDowell Sticks to Recusal Commitment

Despite quasi-green light from GC, Commissioner sits out AT&T/BellSouth vote



By Lee G. Petro
petro@fhhlaw.com
703-812-0453

Citing the Swiss-cheese nature of an ethical opinion letter prepared by the FCC's General Counsel, Commissioner McDowell, fifth in line at the FCC and the critical third Republican on the Commission, decided that the ethical considerations raised by the merger of BellSouth and AT&T prevented him from tendering his vote in the matter.

To fully understand how Commissioner McDowell was put into this situation, it is necessary to go back in time to February, 2006, when McDowell was nominated by George Bush to be the fifth FCC Commissioner. At that time, McDowell served as the Senior Vice President and Assistant General Counsel of COMPTEL. Perhaps emboldened by the idea of three Republicans on the Commission, AT&T announced its plan to merge with BellSouth a mere 28 days later. Citing major concerns with the merger, McDowell's then-current employer immediately came out against the merger.

After consulting with a number of ethics authorities, McDowell declined to vote, observing that the American people deserve officials who operate under the highest of ethical standards.

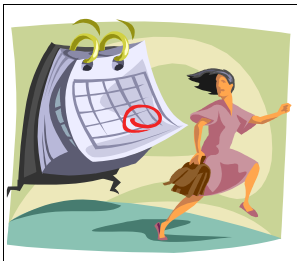
As part of his confirmation, McDowell was required to sign an Ethics Agreement, which prevents him from participating in any proceeding in which COMPTEL is also participant, for one year. McDowell cited this Ethics Agreement when he went onto the Hill for his nomination hearing. Subsequent to taking office, McDowell recused himself from the AT&T-Bell South merger proceeding, as well as other proceedings in which COMPTEL is a participant.

FCC action on the merger was delayed for months by the absence of tie-breaking vote on the merger, pitting the two Republican Commissioners against the two Democrat Commissioners. As a result, on December 1, 2006, Chairman Martin ordered the FCC's General Counsel to determine if the "Government's interests" would be served by McDowell's participation in the meeting.

In response, the Opinion Letter provided by the FCC's General Counsel stated that the balancing act was "difficult" and that reasonable people "could disagree", but that McDowell should not be barred from voting on the matter. Part of the balancing act was a determination whether a "reasonable person" would question McDowell's impartiality. The Opinion Letter focused on the need for an expeditious ruling on the merger between AT&T and BellSouth, and the fact that AT&T and BellSouth did not have a problem with McDowell voting on the merger (no surprise there!). Finally, the Opinion Letter noted the deadlocked nature of the proceeding, and that it was very similar to a past deadlocked proceeding involving former Chairman Kennard and a review of the Commission's personal attack and political editorial rules.

In reviewing the Opinion Letter, McDowell indicated that he had expected that the Opinion Letter would have provided "strong and clear" support for his participation. He noted the hesitant nature of the Letter, and the fact that the Letter failed to even mention the Ethics Agreement, let alone resolve whether the Ethics Agreement prevented his participation. McDowell noted that he spoke with ethics counsel at the Virginia State Bar, and the fact that the Office of Government Ethics had indicated that it would recommend against McDowell participating in the merger proceeding. McDowell concluded

(Continued on page 4)



Next deadline: 2010

Three-Year WCS Build-Out Extension Granted

By Jeffrey J. Gee
gee@fhhlaw.com
703-812-0511

On December 1, 2006, the FCC granted a three year extension of the construction deadline for a large number of Wireless Communications Services (WCS) licenses. WCS licenses authorize operations in the 2.3 GHz band and permit a wide range of wireless services, including fixed, mobile, and radiolocation services. WCS spectrum has been used extensively in other countries for wireless broadband services. In 1997, the FCC granted 126 WCS licenses to operate in the 2305-2320 MHz and 2345-2360 MHz bands. These licenses have a ten-year term, at the end of which WCS licensees must make a showing of "substantial service" in their licensed area. Thus, the build-out deadline for the WCS licenses issued in 1997 was scheduled to end on July 21, 2007.

In their requests for an extension of this deadline, several WCS licensees asserted that matters beyond their control delayed the build-out of WCS services. The central problem confronting WCS licenses is their next-door neighbor, the Satellite Digital Audio Radio Service (SDARS). The two licensees of this service are "satellite radio" providers Sirius and XM Radio. These services sit directly between the two WCS blocks at 2320-2345 MHz. Sirius and XM Radio use this spectrum not only for their satellite distributed signals but also for terrestrial repeaters or "gap-fillers." The satellite radio providers claim these gap-fillers are needed to ensure continuous service in areas subject to signal blockage or multipath interference (*e.g.*, downtown urban areas). The FCC has a pending rulemaking to establish rules and standards for these terrestrial repeaters but, in the meantime, they currently operate under special temporary authority (STA) in several markets.

WCS licensees have long been concerned about the potential interference caused by relatively high-powered adjacent band terrestrial operations. The uncertainty caused by these SDARS operations, the WCS licensees claim, has delayed WCS equipment development, network design and facility deployment. An extension is needed, the WCS licensees argued, to allow the FCC to establish permanent rules and standards for these SDARS operations and allow the WCS services to develop equipment and networks that compensate for the SDARS operations. For their part, Sirius and XM Radio opposed the extension requests, arguing that WCS licensees were aware of the difficulties and risks they would face when they bid on the licenses.

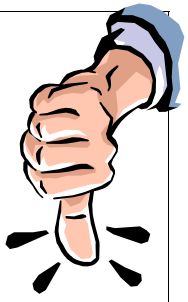
For the most part, the FCC agreed with the WCS licensees and granted three-year extensions to several WCS licensees. The FCC noted that WCS licensees face several technical and equipment problems and therefore have relatively limited options for providing economically viable services. The FCC also noted, however, that new technologies were expected in the near future that would open greater opportunities for WCS licensees. For that reason, the FCC ordered that the three-year extensions would begin at the expiration of the current build out term, rather than the date the SDARS terrestrial repeater rulemaking is completed. The firmer deadline, the FCC reasoned, would push WCS licensees to develop solutions instead of waiting until the rulemaking is complete.

For a list of the licensees affected by the three year extension or for more information about WCS services generally, please contact your communications counsel.

***(McDowell** - Continued from page 3)*
by noting that the American people deserve officials who operate under the highest of ethical standards, and that his recusal will resolve any uncertainty that the four remaining Commissioners will need to work together. With McDowell's participation no longer in issue, AT&T and BellSouth came forward with concessions which they had previously refused to grant. The FCC was then able to unanimously approve the deal on the last day of 2006.

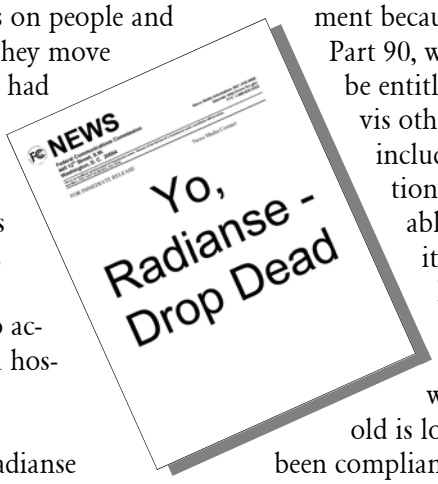
Thumbs down for lo-po doc-tracker

FCC Rejects In-Hospital Positioning System



By Donald J. Evans
evans@fhhlaw.com
703-812-0430

A manufacturer of a low power radiolocation device targeted at locating hospital personnel and equipment was recently rebuffed by the FCC in its attempt to upgrade the device. Radianse's "indoor positioning system" uses tags on people and equipment to track their location as they move around a hospital setting. The device had been certified under Part 15 of the rules to operate on an unlicensed basis but Radianse wanted to increase the time between transmissions from the required 10-second intervals to 2-second intervals. It claimed that the 2-second interval was necessary to accurately track typical movements in a hospital environment.



To avoid the interval requirement, Radianse proposed that its device be operated on a *licensed* basis under Part 90 (the private radio rules) which sets no interval limit, but there it ran into another obstacle – the Part 90 rules impose a higher frequency stability threshold (five parts per million) than the 30 ppm at which the Radianse device operates. The Commission first rejected Radianse's argument that this frequency stability requirement does not apply to low power Part 90 operations such as it proposed; the requirement is frequency-specific rather than power-specific. The FCC also declined to waive the requirement because the device, if operated under Part 90, would have primary status and thus be entitled to interference protection vis-à-vis other users in the 420-450 MHz band, including military radiolocation operations. The FCC did not feel comfortable that the reduced frequency stability would not cause interference. Moreover, the FCC did not see why Radianse could not have chosen a different frequency for its device where the frequency stability threshold is looser and the device would have been compliant (*e.g.*, 150 – 174 MHz rather than the chosen 433.92 MHz).

We always appreciate imaginative theories for skirting the FCC's rules in a good cause, but Radianse's creative approach here unfortunately fell on unreceptive ears.

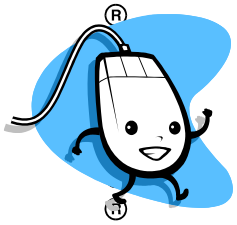
Remnants and returns, up for grabs

On the Auction Block

The FCC will be offering scraps of leftover PCS spectrum in Auction 71, scheduled to commence on May 16, 2007. About 38 licenses (mostly 10 and 15 MHz blocks) which the FCC has not been able to unload or which came back to the FCC due to defaults by earlier buyers will be available. Locations range from American Samoa to Brainerd, MN. A filing date for short form applications should be established shortly.

A similar auction of 220 MHz bric-a-brac will be held on June 20. Ninety-four licenses for 100 kHz blocks in relatively large markets (including Washington, DC) are for sale. All of these came back to the FCC through termination or default by the original holders. Again, the filing deadline has not yet been set.

Guard against theft of your business's identity



Protecting Your Trademark With Just a Click

On-line trademark registration helps overcome cyber squatters

By Kevin M. Goldberg
goldberg@fhhlaw.com
703-812-0462

The maddening thing about technology is it makes almost everything in life easier and harder at the same time. Nearly every administrative personal and business task imaginable can now be accomplished online, from paying bills to renewing vehicle registrations and drivers' licenses to completing your holiday shopping. Broadcast stations have certainly benefited from this through electronic filing of applications via the FCC website. One of the earliest online systems adopted by the FCC was the "Call Sign Registration and Authorization System" which lets broadcast licensees reserve and transfer call signs in a matter of moments. That's it, right? Point, click and go about your business. Anybody in the world can now identify your broadcast station through four easy letters.

But what if others want in? It has often been said that trademarks represent the "blood, sweat, and tears" of the business aspect of an enterprise. Given the amount of time, money and effort that go into promoting a station's call sign as the primary identifier of the business, that station is donating a lot of bodily fluids if others are easily able to incorporate call letters into their marketing efforts.

Given the amount of time, money and effort that go into promoting a station's call sign as the primary identifier of the business, a station is donating a lot of bodily fluids if others are easily able to incorporate call letters into their marketing efforts.

And the "lawless" Internet is the perfect place for someone to try. After all, call signs are short, often catchy, and carry a high rate of recognition in the local market. A radio or television station really only needs one website, right? At the low, low rate of $35 per year, by utilizing the technology-driven simplicity of registering a first-come, first-served domain name over the Internet, isn't it worth it to register a variation of a prominent call sign such as the call plus frequency or call plus station slogan? There is no requirement that the registrant actually use the domain name to create or maintain a website and, in the early days of the Internet, serious compensation was paid – $100,000 for "television.com", for instance – for the rights to very high profile domain names. With a relatively slim chance of being caught, it's worth taking that chance, no?

Broadcast businesses need to police unauthorized use of station call signs and other general business identifiers on a regular basis. Two cases involving trademark infringement through the unauthorized registration of call signs as domain names are particularly illuminating. In one, a radio station in New York used an alternative dispute resolution process to have the rights to two domain names incorporating the station's call sign (www.wevd.com, www.wevd.net) transferred back to the station licensee. These domain names were registered by a former freelance producer who often bought time on the station to broadcast restaurant reviews. He then kindly offered the domain names back to the station in exchange for free airtime during the next five years' "drive time."

The second case is even more frightening. Tennessee station WNRQ used the same procedure to attempt to wrest its call sign from a domain name registrant who was using it to advertise penis and breast enhancement supplements, personal ads, and links to other websites containing sexually explicit materials. Not the sort of thing you want your listeners to encounter when they go searching for your latest contest or station-sponsored events in the community, is it?

The good news is that the Internet Corporation for Assigned Names and Numbers (ICANN), which administers domain names around the world, recog-

(Continued on page 12)

Attention all you website hosts:

Defamation Dangers Decrease

Potential perils of postings petering out

By Ron Whitworth, Law Clerk
whitworth@fhhlaw.com
703-812-0430

With the Internet in constant evolution, increasing in scope and importance, the Federal Communications Commission and courts have struggled to make adjustments in the law to best reflect the rapid technological changes. One of the most hotly contested issues in Internet law is the extent of liability an Internet Service Provider (ISP) should assume for the conduct of its users, and likewise, the individual liability of Internet users for their actions in republishing defamation on the Internet.

In *Barrett v. Rosenthal*, the Supreme Court of California overturned a Court of Appeals decision which was inconsistent with the prevailing interpretation of the Communications Decency Act of 1996 (CDA), in which Congress absolved ISPs from defamation liability. While indicating some discomfort with its decision because of its public policy consequences, the California Supreme Court held that under Section 230 of the CDA, Congress has granted blanket immunization from liability for those who republish defamatory statements. The decision was issued on November 20, 2006. While the decision is controlling only in California, it could have significant precedential value elsewhere.

While indicating some discomfort, the California Supreme Court held that under Section 230 of the CDA, Congress has granted blanket immunization from liability for those who republish defamatory statements.

Traditionally, courts have examined defamation disputes by determining whether a defendant is a "publisher" or a "distributor." "Distributors" such as newspaper vendors or bookstores are liable for defamation only when they have notice of a defamatory statement contained within the materials they distribute. Publishers, however, may be held liable for defamatory content without notice.

Section 230 of the CDA immunizes both ISPs and individual "users" of interactive computer services from liability for defamation, holding "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." In the leading case on Section 230 immunity, *Zeran v. America Online* (1997), the Fourth Circuit provided an extensive interpretation of the CDA, holding that all lawsuits seeking to impose liability on an ISP "for its exercise of a publisher's traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content – are barred."

The Supreme Court of California has now rejected a lower California court's more restrictive interpretation of the CDA and its legislative history. The Court stated that the terms of Section 230(c)(1) of the CDA are "broad and direct," specifically holding that both providers and users of interactive computer services are immune from liability.

In examining the policy considerations involved with the issue, the Court noted that the broad immunity afforded by the CDA can have "some troubling consequences," but the California Supreme Court's interpretation of the statute is contrary to the Court of Appeals' decision. "The prospect of blanket immunity for those who intentionally redistribute defamatory statements on the Internet has disturbing implications," the Court wrote. "Nevertheless, by its terms Section 230 exempts Internet intermediaries from defamation liability for republication." The Court concluded that those who suffer from online defamation can still pursue remedies from the originator of a defamatory publication. But unless and until Congress expands liability beyond the confines of the CDA, as originally interpreted by the *Zeran* court, publishers of content and Internet users will remain shielded from liability for republishing defamatory statements.

In Brief

Adios, Analog? Not so fast – Cellular carriers who have been awaiting the day in February, 2008, when they can finally stop providing analog service now have something else to worry about. (Cellular carriers were required by the FCC to continue to provide service to the very rapidly diminishing population of analog subscribers in order to ensure that those customers, especially the hearing impaired and emergency callers, were not left without service.) ADT (the security alarm service) and something called the "Alarm Industry Communications Committee" have petitioned the FCC to extend the sunset date of the analog service rule for an additional two years. They cite the lack of digital alternatives for the currently analog-based systems which wirelessly connect homes and businesses with alarm centers. The request can be expected to raise protests from carriers who have already been maintaining parallel facilities for several years beyond the point where such service might have been economically justified. Comments are due by January 19, 2007, replies by February 6.

Reef madness – Sometimes in the regulatory world, as in real life, not to decide is to decide. Or, more precisely, not to respond is to respond. Recently a company called Reef Fanatic was sent a couple of official inquiries from the FCC about unspecified behavior. Reef Fanatic apparently did not respond substantively to the FCC's inquiries, though it did acknowledge having received them. The FCC promptly issued a citation to Reef – not for whatever the original behavior was, but for not responding to the inquiry *about* the behavior. The citation included a warning that a further failure to respond immediately would result in up to $11,000 per day in fines. Thus, by ignoring the FCC's original inquiries, the taciturn target made itself potentially liable for a major fine having nothing to do with whether or not it had engaged in any misconduct in the first place. We've said it before and we'll say it again: not responding to these FCC enforcement inquiries is usually not a good strategy. Partially responding may be an even worse one.

(Cells Unlocked - Continued from page 1)

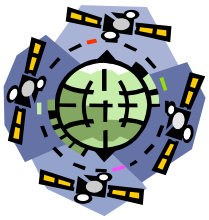
phone could work with to only those that were originally programmed into the phone.

Under the language of the DMCA's anti-circumvention provisions, any attempt to circumvent these "software locks" would constitute a violation of §1201 of the act, regardless of whether there was any underlying copyright concern. After receiving comments from the public requesting that a class of works be created to exempt circumventing these "locks," the Copyright Office exempted "computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network."

Because the DMCA's anti-circumvention provision is meant to supplement private efforts to curb copyright infringement, a key finding in making this exemption was that these "software locks" were *not* being used to protect copyrighted material from infringement. Rather, the "locks" were being used to limit consumer's ability to switch service providers. However, this led to the overly complicated and heavily caveated exemption above. The Copyright Office wanted to make clear that there was no intention to exempt removing these "locks" so that someone could access the cellphones "bootloader" program for the purpose of infringing the copyright of the program's author.

It should also be noted that there was virtually no recognized opposition to creating this exempt class of works. This happy circumstance came about because CTIA (the cellular industry's lobbying group) and TracPhone Wireless did not timely file their opposing comments. Because these comments were filed late, the Copyright Office didn't read or consider them, thereby allowing the rule to take effect virtually unchallenged. TracPhone has since announced, however, that is challenging the new rule in court. If nothing else, this highlights the importance of timely filing in any rulemaking proceeding.

The next Copyright Office exemption rulemaking will take place in the Fall of 2009, and it may behoove people with software gripes to take advantage of the opportunity.



Clowns to the left of them, jokers to the right

DBS Apps Stuck In The Middle

FCC OKs "Tweener" Slots

By Frank Jazzo
jazzo@fhhlaw.com
703-812-0470

The Commission has granted direct broadcast satellite (DBS) applications to EchoStar and Spectrum 5 at short-spaced "tweener" orbital locations. The new DBS satellites are authorized at orbital locations only 4.5 degrees, rather than the standard 9 degrees, from previously authorized DBS satellites. The FCC took action on the applications prior to its completion of a related rulemaking, which proposes the establishment of service rules for DBS satellites at reduced orbital spacing.

Spectrum 5 was authorized to construct, launch and operate two DBS satellites at 114.5°W for the provision of video service to the United States, the Netherlands Antilles and the Netherlands. EchoStar was authorized to construct a new DBS satellite to be operated at 86.5°W. EchoStar will be authorized to launch and operate its satellite once it files a satellite end-of-life disposal plan for its proposed spacecraft.

Both the Spectrum 5 and EchoStar authorizations are subject to any rules adopted in the related "tweener" rulemaking. In addition, Spectrum 5 and EchoStar must coordinate their proposed operations with the currently operating 9 degree spaced DBS satellites. Spectrum 5 will need to coordinate with both EchoStar and DirecTV, since its satellite will be located between DBS satellites operated by the incumbent U.S. DBS operators. Spectrum 5's application was granted over the

(Continued on page 14)

"Fatal Attraction", FCC-style

The Commission's Not Gonna Be *Ignored*

By Mitchell Lazarus
lazarus@fhhlaw.com
703-812-0440

The FCC has been stepping up enforcement against companies that market digital devices. Nowadays this very broad category includes almost every consumer product that uses batteries or wall current – not just PCs and laptops, but also CD players, TVs, cameras, coffee makers, toy dolls, and a staggering array of other items. All of these send out radio waves as an unintended byproduct. Because they have the potential to interfere with radio communications, the FCC has jurisdiction to determine what can lawfully go on sale.

So-called Class A digital devices, which can be used only in commercial and industrial environments, are allowed higher emissions levels and more lenient regulatory procedures. Enforcement against Class A devices is rare. But the FCC recently admonished a company that makes a device having Class A components for overlooking the applicable procedures. The FCC made clear that it would have imposed a monetary fine, had the offenses not predated the one-year statute of limitations

Class B digital devices, which make up the vast majority, are those marketed for use by consumers or in residential areas, or which have mixed consumer and commercial applications (such as PCs). On the same day as its Class A admonition, the FCC imposed a $14,000 fine against a manufacturer of Class B personal computers that were not compliant with the required procedures. That company got off relatively easily. Last February an importer of Class B digital sound equipment was hit with a $1 million fine.

In none of these cases did the FCC allege that the devices actually caused interference, or even that they exceeded the applicable technical standards. The offenses were wholly administrative. To avoid the enforcement action, all these companies had to do was test the product for technical compliance, apply the right labels, and keep certain records. No FCC submission or approval was required.

When dealing with the government, reality does matter, but the paperwork is what really counts.

***(ITU Conference** - Continued from page 1)*

papers. These related to network security and to internet domain names and addresses.

Network Security

Conference Resolution 130 proposed changes to the ITU's role in promoting and preserving security on the telecommunications network. The ITU has traditionally focused on matters related to the physical telecommunications networks. On its face, "network security" relating to the Internet was well within the purview of this organization. However, an active ITU could also negatively impact freedom of the press and freedom of speech on the Internet by allowing ITU Member States (nations of the world) to increase security in the form of "firewalls" which are often used to reduce access to the Internet within domestic borders. While undertaken in the name of protecting critical infrastructures from unsolicited commercial attacks which can cripple the telecommunications network, these security measures can often be put to malicious use by countries seeking to reduce access to the Internet and the exchange of ideas. Adoption of the wrong language relating to network security could also have the adverse result of explicitly condoning some form of content restriction. These fears, while unrealized, were not unfounded.

While undertaken in the name of protecting critical infrastructures, some security measures can often be put to malicious use by countries seeking to reduce access to the Internet and the exchange of ideas.

The initial language of Resolution 130 called for the ITU to support "building confidence and security in the use of ICT's, including ***information and communication network security***" (emphasis added). China – one of the leading innovators/offenders in the use of firewalling to censor speech – tried to identify the ITU's role as consisting of both (1) the technical measures protecting the network itself and (2) the protection of "information security."

Several members of the United States delegation – myself included –recognized this as language that was capable of abuse when put into the wrong hands. Intense discussion and redrafting efforts dragged on for five days as the United States delegation opposed inclusion of the term "information security" and any references to "preventing illicit content" as part of this Resolution.

The debate broke down along rather traditional lines, with the United States facing off against the Russian, Chinese and Cuban delegations over this language. What was lacking was any measure of support for the US point of view from European nations. Most of the Western European democracies should have, on principle, supported the United States; yet, despite my entreaties and those from other members of the United States delegation, many were simply unwilling to undertake any political risk toward that end, instead allowing the United States to shoulder the burden of negotiating this provision. The representative of the United Kingdom eventually spoke out, not in favor of one alternative or another, but simply to state that the effect of the term "information security" could be mitigated "within its mandate" as a qualifier. We had discussed this as an acceptable alternative, but hoped that it would not be the final result.

Just when it looked as though no agreement would be reached, there was a last minute consensus which proved very favorable to keeping the ITU and Member States out of information control. While not the best language, "Strengthening the Role of the ITU in Building Confidence and Security in the Use of Information Communication Technologies" is a positive description of the ITU's future involvement in security issues, as it suggests the ITU will not undertake a formal legislative role but will focus on encouraging technological innovation by Member States.

Internet Domain Names and Addresses

Another important Internet-related issue was the "Management of Internet Domain Names and Addresses," embodied in Conference Resolution 102. In this document, the ITU noted the growth of the Internet as a prime means of communication to fuel knowledge, information exchange and understanding. The ITU's role in this area was widely acknowledged during WSIS. However, Resolution 102 also noted that the growth of the Internet has generally been market-driven by the private sector, and has been left largely to the various countries as well. Thus, the matter of inter-

(Continued on page 11)

*(**ITU Conference** - Continued from page 10)*
net domain names and addresses could be boiled down to two issues:

- Will the ITU try to take an active role for itself or will it simply try to reserve sovereignty for Member States?
- How far will the ITU's reach extend: simply to domain names and addresses or to resources and other management issues as well?

With regard to the first, the ITU limited itself to offering a platform for encouraging discussions and disseminating information with regard to Internet domain name and address distribution. The ITU would continue to assert itself forcefully and supportively in the activities of the Internet Governance Forum and encourage Member States to do the same. Because each nation must have sovereignty over its own Internet domain naming system, countries should be prohibited from interfering with the decisions of other nations.

The latter issue was also resolved favorably. While the ITU could possibly have opened the door to a greater role for itself and individual Member States in all aspects of Internet management, it did not. There was some discussion of concern to the ITU which related to whether this resolution would apply simply to "Internet Domain Names and Addresses" or the broader "Internet Resources." It was a relief when the compromise language "Internet domain names and addresses and other Internet resources within the mandate of ITU" was reached, with the emphasis being that the ITU should stick to telecommunications issues. This was defined by some as "one of the defining issues of the conference." This was accomplished with a remarkable lack of stress and only one late-night meeting of an ad hoc committee on the issue.

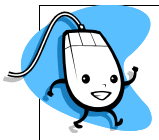
Suggested Responses Begin at the Grass Roots Level

There is no doubt that the ITU will remain involved in Internet governance. It has already scheduled agenda items related to this topic for upcoming conferences that will be held before the next Plenipotentiary in 2010. Thankfully, the ITU recognizes that its role is necessarily limited to that of a facilitator and organizer, not legislator.

It is important that anyone with an interest in continued freedom of speech on the Internet carefully monitor actions by the ITU and other international organizations on international Internet governance. As I learned at the Plenipotentiary Conference, even observers play an important role. The structure of an ITU-related event is such that much of the key drafting and discussion is done on an informal basis, often outside of the organized committee or general sessions at which only the Member States or Sector Members can speak. Thus, anyone with even an indirect role in international telecommunications matters can benefit from having a representative at these events to informally participate in the drafting process. The presence of corporate or non-governmental entities is enough to ensure that those with an official role curtail wide-ranging statements. But the value of experience cannot be overstated – the procedures and protocols in play necessarily relegate those with no first-hand experience at an international conference of this sort to the sidelines.

Anyone with even an indirect role in international telecommunications matters can benefit from having a representative at these events to informally participate in the drafting process. The presence of corporate or non-governmental entities is enough to ensure that those with an official role curtail wide-ranging statements.

Similarly, it is important to be aware of legislative actions at the domestic level, as many nations see no problem with protecting "information" on the Internet. As telephone service and the Internet continue to converge across the world's communications networks, so too will the ability to promote and restrict messages. Those faced with indeterminate language related to security, national sovereignty over the Internet or the role of nongovernmental organizations in promoting a free telecommunications network should feel free to contact me for more advice on how to increase their exposure and impact at the international level.



(**Trademark Protection** - *Continued from page 6)*

nized the danger of allowing anyone in the world to register multiple domain names at a very low price. It is to combat the activities of unscrupulous "cyber squatters" that the "Uniform Dispute Resolution Policy" was created. This is a streamlined, paper-only arbitration process that serves as an alternative to court litigation when unauthorized registration of a domain name is alleged to infringe a federal trademark. In addition to being relatively cheap (usually under $1000 to file a case to be heard by an arbitrator, plus attorney fees) and rapid, a complainant is spared the need to go overseas to prosecute a claim of trademark infringement in the country in which the domain name registrant is located, and victory will result in transfer of the domain name within 10 days of an arbitrator's final order.

More importantly, as opposed to the general federal court standard that amounts to little more than "I'll know it when I see it," the arbitration process is rather concrete and easy to follow. In order to compel transfer of a domain name, the person filing the complaint must show that:

1. The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;

2. The person registering the domain name has no legitimate right to that name; and

3. The domain name has been registered and used in bad faith.

The burden rests with the person bringing the complaint to demonstrate that each of these factors is present. With regard to demonstrating registration in bad faith, this often involves evidence of an attempt by the domain name registrant to sell the trademarked name for a profit, to prevent the trademark owner from using the trademark or to disrupt the trademark owner's business or even piggyback off the trademark for commercial gain. Evidence of the lack of legitimate right to the domain name will often rest on a demonstration that the domain name was never used by the registrant prior to the existence of a controversy over the name, as well as the lack of any connection between the domain name registrant and the trademarked term, other than the registration at issue.

By far and away the most straightforward element of this simple arbitration procedure should be the first one: a federally registered trademark is all the evidence needed to meet this requirement. This is the key difference between the two cases discussed above: WEVD was victorious because it had obtained federal registration for its call sign. WNRQ fell at this first hurdle because it did not have such protection; the station's licensee was forced to demonstrate that its consistent and public use of the call sign amounted to the existence of a common law trademark. The arbitrator disagreed with the station's claim that it met this standard, stating:

> "The granting of a distinctive call sign by the Federal Communications Commission is not a substitute for the granting of a registered trademark by the U.S. Patent and Trademark office. Given the size and population of the United States, there must be many thousands of radio stations with many permutations of letters in their various call signs."

Trademark protection is retroactive to the date of first use of the mark, so even a company that finds itself embroiled in a confrontation over a domain name can file for trademark registration after becoming aware of a cyber squatter.

While the station admittedly offered only scant evidence – in the form of a few "airchecks" to support its claim that it was widely known as "WNRQ" – one thing is clear: the station would not have been required to produce any evidence other than the single-paged trademark registration in order to prove this element, a savings of significant time and money if it had only obtained federal trademark protection for its call sign.

The better news – and, yes, technology is to be lauded once again – is that protecting yourself in this manner is easier than ever. An application for federal trademark protection can be filed online in about an hour for a one-time filing fee of $325.00. Trademark protection is retroactive to the date of first use of the mark, meaning that even a company that finds itself embroiled in a confrontation over a domain name can (and should) file the trademark registration application after becoming aware of a cyber squatter to assert

(Continued on page 13)

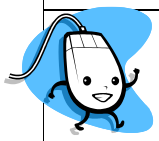
(**E-Discovery** - *Continued from page 2)*
edges that it is impossible to store every bit of electronic data that a firm creates in its day-to-day operations, and that electronically stored information is inevitably overwritten in a routine manner. An example of discoverable, but routinely overwritten, electronic information is "metadata." (Metadata is the information that a computer stores about a document such as the last person who used it, the date it was last modified, etc.) This information, which can be highly relevant to litigation, is often times automatically overwritten every time the document is accessed, and this usually cannot be prevented.

Another example of routinely overwritten electronic data is that which is stored on backup tapes. In general, businesses do ***not*** have a duty to preserve backup tapes for all electronic information related to their business dealings, unless they are aware of potential litigation. Therefore, if it is the general practice of a business to overwrite their backup tapes, or drives, on a weekly basis, there is no duty to preserve the overwritten information until it becomes clear that they may be involved in a lawsuit – and consequently, a litigant will not have sanctions imposed for failing to provide properly requested electronically stored information if this information was lost because of the good faith, routine operation of the litigants IT system.

But be aware, good faith is subjective, and would likely require the litigant to suspend the routine overwriting of information once he/she reasonably becomes aware that the information could possibly be relevant to potential litigation. For instance, if a company routinely overwrites backup tapes once a week, but a contract dispute arises, the overwriting practice should be suspended so that new relevant information pertaining to that dispute is erased. Additionally, it is important to keep up-to-date contact information for former IT managers, as they may be required to give evidence of what the routine business practice was for overwriting, or storing electronic data at some previous time, that happens to be relevant to discovery in an ongoing lawsuit.

It is important to keep up-to-date contact information for former IT managers, as they may be required to give evidence of what the routine business practice was for overwriting, or storing electronic data at some previous time which happens to be relevant to discovery in an ongoing lawsuit.

In a perfect world, none of us would ever get involved in litigation and, thus, none of us would ever have to deal with discovery questions. But since we don't live in a perfect world, there is at least a reasonable chance that, at some point, we will all have to start sorting through our various files in order to answer discovery requests. As the Boy Scouts say, be prepared.



(**Trademark Protection** - *Continued from page 12)*
primacy over the mark. Because a trademark is considered (intellectual) property, it can be transferred in the event that the station is sold or the call sign itself is transferred to a new owner.

Thus, business owners should consider registering their most important commercial identifiers, such as a call sign in the case of a broadcast station or trade names in the case of other businesses, as insurance against spending much more to protect the mark later on when a cyber squatter comes along and tries to shake the business down. It should also engage in regular policing of the Internet, searching for its own call letters, using the "Whois" registry of domain names and owners, and simply typing variations of its call sign into the address bar on its Internet browser in order to remain vigilant against improper uses of a protected mark as an Internet domain name. These searches will prove well-worth the hour or so that is required each month.

We have significant experience in these matters and can assist you in protecting this valuable piece of property. For more information, contact Kevin M. Goldberg (the attorney who represented WEVD in the victorious arbitration discussed above) or the attorney at Fletcher, Heald & Hildreth with whom you usually work .

Fletcher, Heald & Hildreth, P.L.C.
11th Floor
1300 North 17th Street
Arlington, Virginia 22209

First Class

*(**Tweener Slots** - Continued from page 9)*

opposition of both EchoStar and DirecTV. EchoStar will need to coordinate its new satellite with Telesat, which operates the Canadian DBS satellites Nimiq 1 and Nimiq 2 at 91°N and 82°W, respectively, and which had opposed the EchoStar "tweener" application.

Separately, the FCC's International Bureau dismissed the original "tweener" application filed in 2002 by SES Americom (SES) at 105.5°W. SES's original filing did not satisfy the FCC's feeder link cross-polarization requirements. SES was given 30 days to refile a compliant proposal and trade press reports indicated SES will do so.

And last but not least, a

Report from Planet FCC

A decade here, a decade there . . . pretty soon you've got a real delay. The FCC recently issued an order directing the processing of a Broadband Radio Service renewal application which had been filed in May of 1996. The problem was that the licensee had filed the renewal application 16 days after the deadline but before the license actually expired. After mulling the matter over for ten and a half years (!), the FCC decided that, although it could not condone the 16-day late filing, the lateness "did not unduly disrupt consideration" of the renewal. Phew. One can only imagine how long the process would have taken if there actually *had* been an undue disruption. In any event, the application has now been restored to the processing line and, if there are no undue disruptions, we can anticipate routine approval sometime around 2017.