Message from the Chair

Michael Fleming
Chair, Committee on Cyberspace Law

The pages of the calendar turn whether we like it or not, and the warm glow of a successful Annual Meeting in New York City is rapidly being overtaken by the blinding flash of a Winter Working Meeting in just a few more days! After a January, 2008 WWM in the Twin Cities that 'put the winter back,' we return to warmer climes in Santa Clara, California on the campus of Santa Clara University, hosted by the High-Tech Law Institute - January 30 and 31. You will see links to the meeting notice page in this newsletter - Please sign up and get your tickets as soon as you can!

WWM is your annual opportunity to browse amongst the various offerings of the Committee, connect with a new project or two, and network with members who share your interests. You may already be involved in a matter and will be going with a specific task in mind, or you may be going with the idea to contribute to something new or to meet people. You may be going to your tenth (or more!) winter meeting, or this may be your first. In any event, you are more than welcome to join us, as this is our roll-up-your-sleeve event with no expectations other than helping us to move our missions forward.

The coming year looks like another great one for CLCC, with a slate of new books coming down from ABA publishing authored by members of our Committee, a presentation slated for the Business Section's Global Business Law Forum in Hong Kong sponsored by Cyberspace Law as well as the Corporate Compliance Committee, enough programs we'll be sponsoring or heavily involved with at the upcoming Vancouver, BC Spring Meeting that you'll need more than one hand to count them, and an Annual Meeting in Chicago this Summer that we are still looking to plan! The Committee maintains its prominence in the ABA as a leading resource on data privacy and security issues, Internet governance, electronic financial systems, electronic contracting and e-commerce, consumer protection, intellectual property, Web 2.0, and... I could go on, but you would do better to check out the listings of various subcommittees, task forces and working groups that comprise the Committee's substantive forces. See our Committee Home Page for more information. (Speaking of the Home Page - I am looking to recruit a person to be our committee's 'webmaster' for the home page and various sub-pages. This is a great opportunity for a newer member, with web skills or a willingness to learn a bit, to be part of the Committee's leadership. Contact me if you are interested!)

Please take a moment to welcome our new Committee leaders when you can, and let them know how you want to participate in our activities and work product. Christina Kunz and Lisa Lifshitz are newly installed as co-Vice-Chairs of the Committee, Juliet Moringiello is maintaining her position as Publishing Director, Jonathan Rubens is the new Programs Director, and Susan Stephan is taking over on Membership. We have one new position on the Committee-level leadership, the Newsletter Director, and Alan Wernick has begun that with the publication of this new eNewsletter you are reading today.

The newsletter is where we will publish news from the business of the Committee and its sub-groups, including meeting notices, requests for assistance, announcements of new projects, and so forth. We also want to give all of our members, including those who aren't as able to attend our in-person meetings, a forum to publish short substantive articles. See examples in this
Thank you for being members of one of the biggest and most dynamic committees in the ABA's Section of Business Law - I look forward to seeing or hearing from all of you!

Message from the Newsletter Director

**Alan S. Wernick**  
Newsletter Director

The Committee on Cyberspace Law explores a wide range of rapidly changing legal disciplines including electronic commerce and contracts, consumer protection, intellectual property, cyber security & privacy, jurisdiction, internet governance, and online financial activities. This CCL eNewsletter provides our members with an opportunity to help advance members' awareness and understanding of these evolving and dynamic legal issues. Our goal is to make it a useful addition to your practice by helping to make you aware of some of the developments impacting your practice and your clients' businesses, and what these developments mean. Please contact me if you are interested in submitting short articles for publication in this eNewsletter, or if you have any constructive comments or suggestions concerning this newsletter.

Thanks to our contributors for this issue: Jeff Aresty, Amy Boss, Kristine Fordahl Dorrain, Michael Fleming, and Christina Kunz.

In Memory of Prof. Donald F. Clifford, Jr.: Celebrating His Contribution to Consumer Protection Online

**Amy Boss and Christina Kunz**

On October 19, 2008, we lost our dear friend and dedicated colleague, Prof. Donald F. Clifford, Jr. As you sit at your computers searching for the perfect gift for holidays, birthdays, and other special occasions, please remember Don and one of the most significant and visible works created for the Cyberspace Committee under his leadership: the 2005 overhaul of SafeShopping.org. SafeShopping.org offers tips and information for consumers who choose to shop online, and it has been a valuable resource for consumers as they adapted to the new commercial environment.

As many of us in the Committee helped our business clients move commercial transactions online, Don contributed his knowledge of consumer protection law to our efforts. Don's advocacy challenged us to consider issues that could have been easily overlooked or ignored, and in doing so, Don helped make the Committee's projects richer and more accessible to a wider audience. Don will be especially missed in the Committee because few consumer advocates are both willing and able to...
participate regularly in Business Law Section activities. As we continue to lead the way in the combination of business law and emerging technology, we should follow Don's example and consider how our work will impact the rights and responsibilities of individual consumers. The result will be a more solid legal foundation to support those new business opportunities.

While many of us know Don through his work with the Cyberspace Committee, Don was a long-standing active member of the UCC Committee as well. Don was a key member of the team of ABA Observers to the UCC Article 2 redraft process, run by the National Conference of Commissioners on Uniform State Law (NCCUSL). Over the eight-year period in which the NCCUSL Drafting Committee met 3-4 times per year, he attended almost every meeting and made extensive written and oral comments to the Drafting Committee. His knowledge and insight into the Article 2 warranties were especially valuable, and, among the ABA Observers, he became the "go-to guy" on warranty issues. He also joined his fellow ABA Observers on yearly panel presentations that updated practitioners on the redraft process. His scholarly observations about Article 2 were always carefully supported by his vast knowledge of the case law and the full range of commercial and consumer applications.

Don's contributions were far more than substantive. Don was a wonderful mentor and role model for all with whom he worked. Truly dedicated to the improvement of the law and the protection of those who could not protect themselves, Don was a model of integrity and at the same time humility.

Don taught at the University of North Carolina - Chapel Hill School of Law, beginning in 1964, where he was the Aubrey L. Brooks Professor Emeritus. Don's classes included business associations, sales, secured transactions, consumer law, and a seminar on State Laws of Unfair and Deceptive Acts and Practices. In recent years, as a result of his work in the Cyberspace Committee, Don consulted with the American delegation on consumer protection proposals in an Organization of American States project involving Brazil, Canada and the United States.

Don is survived by his wife Louise, five daughters, and many grandchildren. Please keep Don's family in your thoughts and prayers.

**Featured Articles**

**The PeaceTones Initiative**  
*Jeff Aresty, President, The Internet Bar Organization*

The Internet Bar Organization ("IBO") is pleased to announce the receipt of a grant from the American Bar Association Fund for Justice and Education, through the World Justice Project, for its PeaceTones Initiative. The PeaceTones Initiative addresses the isolation of individuals in conflict zones and zones recently freed from conflict. Prolonged conflict serves as an anchor, holding back populations that are vandalized and deprived of resources, populations living at or below the international poverty line, and populations that are overlooked or exploited by local governments. PeaceTones aims to assist musicians and their communities in
conflict and post-conflict zones with access to Internet technology, legal assistance in establishing and maintaining intellectual property rights, alternative dispute resolution assistance to ensure successful ongoing development, and business assistance to bring remote market prices to local developing markets. IBO will ensure that the proceeds from these sales go directly to the musicians and/or their cooperatives, but retains a portion of the money received pursuant to the draft of the PeaceTones Artist Agreement. The legal community’s role in PeaceTones is to design and build-out an international legal empowerment network, including a user interface, comprised of lawyers from all over the world who donate their time and expertise to help advise artistic individuals who otherwise would not have access to rule of law due to monetary or location based restriction. For more information see: [www.peacetones.org](http://www.peacetones.org).

The Liberty Alliance, a standards organization with a global membership that provides a holistic approach to identity, is collaborating with the legal community to develop a system of legal assurance for identity within the legal empowerment network. The PeaceTones Initiative will be but one place their work will be used. The vision of Liberty Alliance is to enable a networked world based on open standards where consumers, citizens, businesses and governments can more easily conduct online transactions while protecting the privacy and security of identity information. For more information see: [www.projectliberty.org](http://www.projectliberty.org).

The launch of the PeaceTones legal empowerment network will take place at the Winter Working Meeting of the Cyberspace Law Committee of the ABA Business Law Section from January 30-31, 2009 at Santa Clara University.

About The Author: Jeff Aresty is the President of The Internet Bar Organization.

Online contracts—Take notice!

*Alan S. Wernick*

Every time you visit an Internet site you most likely are agreeing to be bound by the terms and conditions associated with that website, including subsequent revisions. Or are you?

Most sophisticated websites include a “terms and conditions” page accessible by hyperlink from the home page and from nearly all of the other pages of the website. This is particularly true if the website offers goods and/or services. However, there are many other websites that include (or should include) terms and conditions as an integral part of the site: health care providers, education, newspapers, libraries and other public institutions, professional organizations, trade associations, and government entities, to name a few.

More...

*When Can A State Seize Domain Names In Rem?*

*Kristine Fordahl Dorrain*

Does a state court have jurisdiction to seize domain names registered by non-United States individuals simply because the domain name registrants have websites that are freely accessible throughout the world? Should domain name registrants be
expected to face lawsuits in any locale where their website might be accessed? Which laws apply to a domain name registrant as they set up their website? These questions have been touched on, skirted, and addressed by a variety of United States courts, but none with quite so much audacity as a circuit court in Kentucky.

In September 2008, Judge Wingate for the Franklin Circuit Court in the Commonwealth of Kentucky, in Commonwealth of Kentucky ex rel. Brown v. 141 Internet Domain Names, No. 08-CI-1409. (KY Cir. Ct. 2008), took unprecedented steps to enforce Kentucky’s statewide gambling ban. In an ex parte hearing, the Commonwealth requested that the Court seize 141 Internet Domain Names for alleged connections to online gambling services available to the residents of Kentucky. The Court agreed to the Commonwealth's request on September 18; the "seizure" consisted of an order to transfer registrations for the 141 Internet Domain Names to the Commonwealth's accounts. After additional amici entered the litigation, further hearings were held. The court then issued its Opinion and Order on October 16, 2008, allowing the seizure.

More...

SCA and 4th Amendment Trump Employer's "Computer Usage, Internet and E-mail Policy"
Alan S. Wernick

In Quon vs. Arch Wireless Operating Company, Inc., et al., (June, 2008), the United States Court of Appeals, 9th Circuit, sounds another warning to employers and highlights the risks of a disconnect between conditions stated in an employer's "Computer usage, Internet and E-mail policy" (the "Policy") and the actual practices of the employer.

The Quon case involved several police officers (the Appellants) who were issued pagers by their employer, the Ontario (California) Police Department ("OPD"), and who used the pagers for personal text message communications. OPD had contracted with Arch Wireless Operating Company, Inc. ("Arch Wireless") to provide text messaging service. As part of OPD's auditing of the bills for the text messaging service, OPD requested that Arch Wireless provide OPD copies of the text messages sent by the Appellants, some of which messages were "personal in nature and often sexually explicit." The Court first addressed whether Arch Wireless violated the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2711 (1986), and concluded Arch Wireless did violate the SCA, and then addressed whether the Appellants' rights under the 4th Amendment were violated, and concluded that the employer did violate the employees' 4th Amendment rights.

More...
Online contracts—Take notice!
By Alan S. Wernick

===============
Editor’s Note: The Cyberspace Law Committee has been examining issues surrounding online contracting for many years. At the ABA Annual Meeting in 2007, members Eran Kahana, Christina Kunz, Juliet Moringiello, John Ottaviani, and Kathleen Porter, presented on this issue to assembled members. Copies of their program materials can be found at http://www.abanet.org/buslaw/mo/premium-cl/programs/ann07/11.pdf (Business Section Membership required).
===============

Every time you visit an Internet site you most likely are agreeing to be bound by the terms and conditions associated with that website, including subsequent revisions. Or are you?

Most sophisticated websites include a “terms and conditions” page accessible by hyperlink from the home page and from nearly all of the other pages of the website. This is particularly true if the website offers goods and/or services. However, there are many other websites that include (or should include) terms and conditions as an integral part of the site: health care providers, education, newspapers, libraries and other public institutions, professional organizations, trade associations, and government entities, to name a few.

Indeed, some state statutes require that some terms and conditions be posted on the website.

The California Online Privacy Protection Act of 2003, for example, requires commercial websites and online services that collect personal information from California residents to have a privacy policy conspicuously on the site. The statute also sets forth certain
requirements for the privacy policy. Let’s assume that a website follows best practices with its terms and conditions page and sets forth a reasonably sophisticated online agreement. When can unilateral changes to these online contracts be binding? This question was recently addressed by two different courts, resulting in two different outcomes turning on one critical fact — notice.

In *Douglas vs. Talk America, Inc.*, the U. S. Court of Appeals for the Ninth Circuit reviewed an online contract that Talk America, a telecommunications provider, unilaterally changed in several material ways by adding four provisions to the services contract: (1) additional service charges; (2) a class-action waiver; (3) an arbitration clause; and (4) a choice-of-law provision pointing to New York law.

After the plaintiff, a customer for four years, discovered the additional services charges, a class-action lawsuit was filed disputing the charges, among other things. Talk America moved to compel arbitration and the trial court agreed.

However, the Ninth Circuit disagreed. Underscoring the fact that online contracts are still contracts and must adhere to the requirements of contracts, the court stated: “Indeed, a party can’t unilaterally change the terms of a contract; it must obtain the other party’s consent before doing so … This is because a revised contract is merely an offer and does not bind the parties until it is accepted … And generally ‘an offeree cannot actually assent to an offer unless he knows of its existence.’”

The court observed that even if the plaintiff’s continued use of the defendant’s service could be considered assent, such assent can only be inferred after the plaintiff received proper notice of the proposed changes, and the plaintiff claimed that no such notice was given.
In contrast—and highlighting the factual nature of the analysis — the U.S. District Court for the Middle District of Alabama found enforceable contract terms posted on another plaintiff’s website and clearly referenced in the terms and conditions of the website.

In Conference America Inc. v. Conexant Systems, Inc., the defendant was previously a “high volume, preferred customer” of the plaintiff’s services who, because of the high volume, enjoyed discounted call rates subject to a signed written price protection agreement. The plaintiff sent a termination letter to the defendant terminating the price protection agreement, and stated that the plaintiff’s services terms and conditions were available at [the plaintiff’s website], and that the terms and conditions had been revised subsequent to the earlier price protection agreement. These terms included a deactivation fee (not mentioned in the written price protection agreement) among other charges in the event of termination.

The defendant continued to use the plaintiff’s services for several weeks after the effective date of termination in the plaintiff’s termination letter.

Through e-discovery, an internal e-mail revealed that the defendant was aware of the revised terms posted on the plaintiff’s website. Furthermore, the correspondence indicated that the plaintiff referred to the website pricing repeatedly as a condition of its performing services after termination. The court held that the defendant was bound to the terms and conditions posted on the plaintiff’s website and entered a judgment in favor of plaintiff for nearly $200,000, plus reasonable expenses and attorneys’ fees.

In each of these cases, the website had an online contract in which unilateral changes were made to the terms and conditions of that online contract. However, in one case the revised online contract was enforceable and, in the other, it was not, with notice being the critical factor.
Many enforceable statutory obligations are invoked each time you visit a website (for example, copyright laws that govern what you can and cannot do with the content of the site, or the Uniform Electronic Transactions Act, variations of which have been adopted by many jurisdictions). The bottom line is that you need to consider many factors (in addition to notice) not only in the creation of the online contract, but in the unilateral revisions to that agreement, in order to create a binding and enforceable agreement.

© Alan S. Wernick. WWW.WERNICK.COM

About The Author: Since 1982 Alan S. Wernick has been practicing computer law / cyberspace law / information technology law, and intellectual property law. He has a background in computer programming and accounting. Additional information is available at WWW.WERNICK.COM.
When Can A State Seize Domain Names *In Rem*?

By Kristine Fordahl Dorrain

==================

*Editor’s Note: On January 20, 2009, the Kentucky Court of Appeals granted the petitioners’ and amici’s requests to overturn the trial court’s ruling authorizing the seizure by the Commonwealth of Kentucky of domain names owned by operators of gambling websites located outside of the Commonwealth of Kentucky. *Interactive Media Entertainment and Gaming Association v. Wingate ex rel Kentucky*, 08-CI-01409 (Ky. Ct. App. Jan. 20, 2009). Nonetheless, the story below remains relevant, as we cannot know that other jurisdictions, in or out of this country, will not go down this path again.*

==================

Does a state court have jurisdiction to seize domain names registered by non-United States individuals simply because the domain name registrants have websites that are freely accessible throughout the world? Should domain name registrants be expected to face lawsuits in any locale where their website might be accessed? Which laws apply to a domain name registrant as they set up their website? These questions have been touched on, skirted, and addressed by a variety of United States courts, but none with quite so much audacity as a circuit court in Kentucky.

In September 2008, Judge Wingate for the Franklin Circuit Court in the Commonwealth of Kentucky, in *Commonwealth of Kentucky ex rel. Brown v. 141 Internet Domain Names*, No. 08-CI-1409, (KY Cir. Ct. 2008), took unprecedented steps to enforce Kentucky’s statewide gambling ban. In an *ex parte* hearing, the Commonwealth requested that the Court seize 141 Internet Domain Names for alleged connections to online gambling services available to the residents of Kentucky. The Court agreed to the Commonwealth’s request on September 18; the “seizure” consisted of an order to transfer registrations for the 141 Internet Domain Names to the Commonwealth’s
accounts. After additional amici entered the litigation, further hearings were held. The court then issued its Opinion and Order on October 16, 2008, allowing the seizure.

The seizure by Kentucky raises profound implications for the concept of in rem jurisdiction over Internet domain names and the governance of the Internet in general. The facts, and the Court’s order, have raised significant concerns among those lawyers who advise clients on Internet domain names. If allowed to proceed, the forfeiture would upset a number of commonly-held understandings about the powers of states to act on domain names, and the businesses that use them, even when located entirely outside of the state’s borders.

The court, in its October 16th opinion, found that it has subject matter jurisdiction over the civil forfeiture claim because Kentucky law prohibits gambling in the Commonwealth, the 141 Internet Domain Names are being used for online gambling that is accessible within the Commonwealth, and the statute authorizes forfeiture of gambling devices.

The court further found that the 141 Domain Names are property and that they have a “presence” in Kentucky; they are therefore subject to in rem jurisdiction. Certainly, in this case, no domain name registries, registrars or registrants are to be found in Kentucky. Judge Wingate relies on Shafer v. Heitner, 733 U.S. 186 (1977), for the proposition that in rem jurisdiction is subject to the fairness standard articulated in International Shoe Co. v. Washington, 326 U.S. 310 (1945), and that in rem jurisdiction is now subject to a “minimum contacts” review. The court’s logic indicates that, because domain names are property and domain name owners make those domain names resolve to content available online without restrictions, in rem jurisdiction exists in whatever location the website may be viewed.
Assuming that *in rem* jurisdiction, post *Shafer*, requires a “minimum contacts” analysis, a California court noted, of minimum contacts, in 1996:

Because the Web enables easy world-wide access, allowing computer interaction via the web to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently stands; the Court is not willing to take that step. Thus the fact that [defendant] has a website used by Californians cannot establish jurisdiction by itself.


Lawyers and governments around the world certainly act as if the court in the California case is correct. For instance regimes in the rest of the world, in seeking to prohibit access to material protected by our Constitution, but illegal elsewhere (such as political speech, women’s rights issues, pornography, and historical information) have learned to deny their citizens access to a variety of content the regimes find objectionable.

The court mentions the notion raised in *International Shoe* and again in *Shafer* regarding a “reasonable expectation of being hauled into court,” but does not identify how a website operator halfway around the world, participating in an activity legal in his home country, could reasonably expect to be hauled into a court in the United States. Such a person would not have that “reasonable expectation” any more than a Kentucky website operator would expect to have his domain name seized by a Chinese court for posting a true historical account of the massacre at Tiananmen Square in violation of Chinese law.

On October 22, 2008, *amicus* Interactive Media Entertainment and Gaming Association filed an Appeal requesting an Original Proceeding with the Commonwealth of Kentucky Court of Appeals against Judge Wingate, the Commonwealth, and Jack Conway, Attorney General for the Commonwealth, and asking for a stay of Judge Wingate’s October 16, 2008. Amici include the Electronic Frontier Foundation, the Center for

About The Author: Kristine Dorrain is an attorney with Forthright and manages the domain name dispute resolution program for the National Arbitration Forum. This article reflects Kristine’s views only and does not reflect the views of Forthright, the National Arbitration Forum or any ABA Committee. Kristine thanks Michael Fleming and Warren Agin for their assistance and review of the finer points of this article.
SCA and 4th Amendment Trump Employer’s “Computer Usage, Internet and E-mail Policy”
By Alan S. Wernick

In *Quon vs. Arch Wireless Operating Company, Inc., et al.*, (June, 2008), the United States Court of Appeals, 9th Circuit, sounds another warning to employers and highlights the risks of a disconnect between conditions stated in an employer’s “Computer usage, Internet and E-mail policy” (the “Policy”) and the actual practices of the employer.

The *Quon* case involved several police officers (the Appellants) who were issued pagers by their employer, the Ontario (California) Police Department (“OPD”), and who used the pagers for personal text message communications. OPD had contracted with Arch Wireless Operating Company, Inc. (“Arch Wireless”) to provide text messaging service. As part of OPD’s auditing of the bills for the text messaging service, OPD requested that Arch Wireless provide OPD copies of the text messages sent by the Appellants, some of which messages were “personal in nature and often sexually explicit.” The Court first addressed whether Arch Wireless violated the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2711 (1986), and concluded Arch Wireless did violate the SCA, and then addressed whether the Appellants’ rights under the 4th Amendment were violated, and concluded that the employer did violate the employees’ 4th Amendment rights.

The 9th Circuit held that Arch Wireless is an “electronic communication service” (“ECS”) under the SCA, §§ 2701-2711 and liable to Appellants for violating the SCA. The Court stated that “An ECS is defined as ‘any service which provides to users thereof the ability to send or receive wire or electronic communications.’ 18 U.S.C. §2510(15). On its face, this describes the text-messaging pager services that Arch Wireless provided. Arch Wireless provided a ‘service’ that enabled Quon and the other Appellants to ‘send or receive ... electronic communications,’ i.e., text messages.” After further analysis of the
SCA the Court concludes: “When Arch Wireless knowingly turned over the text-messaging transcripts to the City, which was a ‘subscriber,’ not ‘an addressee or intended recipient of such communication,’ it violated the SCA, 18 U.S.C. §2702(a)(1). Accordingly, judgment in Appellants’ favor on their claims against Arch Wireless is appropriate as a matter of law, and we remand to the district court for proceedings consistent with this holding.”

In determining the 4th Amendment issue, the Court focused on the facts (a) that OPD had a written Policy, in which it did not specifically address pagers; and (b) that the policy stated that OPD had the right to monitor, but in fact the Appellants were told (the “informal policy”) that as long as they paid the cost for extra messages over a stated amount in OPD’s agreement with Arch Wireless, OPD would not audit their usage.

In finding that OPD’s search of the pager records was unreasonable as a matter of law, the Court states that “The Fourth Amendment protects the ‘right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.’ U.S. CONST. amend. IV. … [T]he touchstone of the Fourth Amendment is reasonableness.’ … ‘The reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.’” The Court noted that just because Appellants worked for the government, they did not lose their 4th Amendment rights.

In examining the Appellant’s reasonable expectation of privacy, the Court states “The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.” In finding that users of text messaging services have a reasonable expectation of privacy in messages stored on their service provider’s network, the Court analogized the privacy of the text messages to the privacy expectations of a person who
enters a phone booth and closes the door behind him, and the privacy expectations that someone has against the warrantless opening of sealed letters and packages addressed to her in order to examine the contents. The 9th Circuit found support for its finding of a reasonable expectation of privacy in all of these media of communications (i.e., the phone booth and the sealed letter), and thus in the application of the 4th Amendment’s reasonable expectation of privacy in text messaging services.

Most companies today have (or should have) policies with appropriate terms and conditions concerning data privacy and security issues involving computer usage, Internet, e-mails, and other corporate communications systems on or in which the company’s business data travels or is stored for archival or backup purposes. Not uncommon it these policies is a right of inspection by the employer. Indeed, Judge Posner in *Muick v. Glenayre Electronics*, (United States Court of Appeal, 7th Circuit, 2002), states “The laptops were Glenayre's [the employer’s] property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.”

Now, before you find yourself having to defend the policy, is a good time to review your organization’s policies concerning employees’ use of computers, Internet, e-mail and other communications technologies, the periodic training that should go along with those policies, and the periodic legal audit to check for compliance.

© 2008 Alan S. Wernick.  WWW.WERNICK.COM

About The Author: Since 1982 Alan S. Wernick has been practicing computer law / cyberspace law / information technology law, and intellectual property law. He has a
background in computer programming and accounting. Additional information is available at WWW.WERNICK.COM.