



# FEDERALLY SPEAKING



by Barry J. Lipson

## INTERNET & COPYRIGHT COMPILATION ISSUE

*The Western Pennsylvania Chapter of the Federal Bar Association (FBA), in cooperation with the Allegheny County Bar Association (ACBA), brings you Federally Speaking*

### Fed-pourri™

**CYBERSQUATTERS BEWARE, JOE CARTOON IS HERE!** The U.S. Congress has enacted the **Anticybersquatting Consumer Protection Act (ACPA) of 1999** (15 U.S.C. Sec.1125 (d)). Cybersquatting is “the bad faith, abusive registration and use of the distinctive trademarks of others as Internet domain names, with the intent to profit from the goodwill associated with those trademarks” (**Shields v. Zuccarini**, No. 00-2236 (3d Cir. June 15, 2001)). The **ACPA** makes “it illegal for a person to register, or to use with the ‘bad faith’ intent to profit from, an Internet domain name that is ‘identical or confusingly similar’ to the distinctive or famous trademark or Internet domain name of another person or company,” and imposes a penalty of from \$1,000 to \$100,000 per domain name (15 U.S.C. Sec.1117 (d)). Now, Joe Cartoon has shown you cannot squat on him! Joe Cartoon, a/k/a Joseph C. Shields, a graphic artist, creates, exhibits and markets cartoons under the names "Joe Cartoon" and "The Joe Cartoon Co.," and does so, in part, on the web through the registered domain name “joecartoon.com.” In April 1998 this site won the Macromedia "Shock Site of the Day" Award, whereupon “Joe Cartoon's web traffic increased exponentially, now averaging over 700,000 visits per month.” Apparently sensing another “Jessica Rabbit” bonanza, one Andalusia, Pennsylvania cyber-opportunist and "wholesaler" of Internet domain names, John Zuccarini, “registered five world wide web variations” of Joe’s name, “joescartoon.com, joecarton.com, joescartons.com, joescartoons.com and cartoonjoe.com.” Upon taking this bait, the unwitting and/or poor spelling surfers were, “in the jargon of the computer world ... mousetrapped,” or, in regular English, “they were unable to exit without clicking on a succession of advertisements.” And each desperate click netted Zuccarini “between ten and twenty-five cents from the advertisers.” In affirming the **U.S. District Court’s** grant of **Summary Judgment** and award of \$50,000 in statutory damages, and “punitive” attorneys' fees, in favor of Joe, the **U.S. Court of Appeals for the Third Circuit** concluded that, while not involving “pornography,” the gentleman from Andalusia’s “conduct here is a classic example of a specific practice the **ACPA** was designed to prohibit,” the registration of domain names that are "confusingly similar," thus clearly including "typosquatting" within the ambit of the **ACPA**. The squatter Zuccarini didn’t know “squat,” did he?

**Doppelganger Protection Act.** Webster defines a doppelganger as “a ghostly copy of a living person.” We define it here as a “non-material or ‘ghostly’ electronic copy of a living (still under **Copyright**) paper article.” Justice Ginsburg, writing for the 7-2 majority of the **U.S. Supreme Court**, has rejected the notion

that such a “Doppelganger,” also know less colorfully as an “electronic database copy,” remains covered by the **Copyright** on the print edition of the newspaper or magazine, as being still part of a statutorily permitted revision of that original print edition. She based her finding primarily on the fact that the typical database user, such as LEXIS/NEXIS users, did not retrieve an entire newspaper or magazine, but merely the individual article that was sought. Materializing from the Nether Realm the nebulous “**Doppelganger Protection Act**,” the **High Court** therefore held that, without the author’s permission, a newspaper or magazine publisher is barred by the **Copyright Act** from distributing such Doppelgangers of its freelance print articles through electronic databases (New York Times v. Tasini, 69 U.S.L.W. 4567, June 25, 2001).

**DIGITAL WARS AND FAIR USE.** The **Digital Media Consumers Rights Act of 2002 (DMCRA)** was recently introduced in **Congress** by Representatives Rick Boucher (D-VA) and John Doolittle (D-CA), as a counterattack in the “Digital Media Wars,” to preserve the time-honored **Doctrine of Fair Use** in the field of technologically “protected” digital/electronic works, and to permit the circumvention and bypassing of technological protection measure that allegedly have annihilated “fair use” in this battlefield. The aggressor, according to this Bill’s proponents, the “Entertainment/Recording Industry,” purportedly had such “fair use” outlawed through its massive lobbying campaign, which brought about the 1998 enactment of the **Digital Millennium Copyright Act (DMCA)**. “We all employ the **Fair Use Doctrine** in everyday life,” advised Rep. Boucher. “From the college student who photocopies a page from a library book for use in writing a report to the newspaper reporter who excerpts materials for a story, to the typical television viewer who records a broadcast program for viewing at a later time. ... The **Fair Use Doctrine** was fashioned by the **federal courts** as a means of furthering the vital free expression values that are given constitutional recognition in the **First Amendment**. ... It permits limited personal non-commercial use of lawfully acquired **copyrighted** material without the necessity of having to obtain the prior consent of the owner of the **copyright**,” such as the use of this quote here, if the Representative’s remarks had been **copyrighted**. He further contends that the “unfairness” of this crippling of the **Fair Use Doctrine** has already surfaced in litigation and threatened litigation forays, citing *Elcomsoft* and *Felten*. In *U.S. v. ElcomSoft and Dmitry Sklyarov* (NDCA, CR-01-20138RMW), “a Russian software manufacturing company is being prosecuted before a federal court in the United States” on criminal charges for making software that enables the lawful owner of an electronic book “to make a back-up copy,” because the software must circumvent “the technical protection measure guarding access to the text of the electronic book.” While Adobe, the producer of the subject “e-books,” has abandoned its civil suit, the Government has advised your columnist that it will continue the criminal prosecution of Elcomsoft in the **U.S. District Court for the Northern District of California** (though not defendant Dmitry Sklyarov, the Russian programmer the Government had arrested and indicted when he visited the U.S., if he continues to cooperate). In *Felten, et al. v. RIAA, SDMI, Verance Corp., John Ashcroft, in his Official Capacity as Attorney General Of the U.S., et al.* (DCNJ, CV-01-2669GEB), Edward W. Felten, a “tenured professor of computer science” at Princeton University, and a key Government witness in *U.S. v. Microsoft* (his testified about software he developed to remove the Microsoft web browser from the MS Windows operating system), “enters a contest to defeat watermarking technology that will be used to protect against the redistribution of audio content.” Then, according to the Electronic Frontier Foundation (EFF), in doing so “Professor Felten and a team of researchers from Princeton University, Rice University, and Xerox discovered that digital watermark technology under development to protect music sold by the recording industry has significant security vulnerabilities. The recording industry, represented by the **Recording Industry Association of America (RIAA)** and the **Secure Digital Music Initiative (SDMI) Foundation**, threatened to file suit in April 2001 if Felten and his team published their research at a conference.” Felten and his team thereupon sought a **Declaratory Judgment** in the **U.S. District Court for the District of New Jersey** against **RIAA, SDMI, Attorney General Ashcroft** and others, based upon their **First Amendment** free speech rights, and only abandoned this litigation when the defendants agreed not to bring legal actions under the **DMCA** for their making this research public. Ironically, the Record Industry’s threat of suit was made “by the very organization that sponsored the contest.” It appears likely that a hotly

contested key battle in these Digital Wars will be fought on **Capital Hill** next session. Hopefully, “fairness” and the **Constitution** will prevail. Also, this term, the **U.S. Supreme Court** will be deciding if “the author’s life plus 70 years” is the “limited” **copyright** contemplated by the **U.S. Constitution**.

**CORPORATE COUNSELS HEADS UP!** From years of corporate counseling it has been a “rule of thumb” that if you want the **Government** to bring a case they won’t, and if you don’t want the case brought they will! During my **Food, Dug and Cosmetic** days, I vividly remember amassing a case full of vivid “passing off” examples, by a major interstate supermarket chain, of private label groceries with label designs and coloring virtually identical to the brand name products (including those of my client), and shipping this case with a detailed analysis to the **FTC**. The **FTC**, of course, kept the case of groceries, while rejecting the legal case. But times may be a changing! In *U.S. v. ElcomSoft and Dmitry Sklyarov* (NDCA, CR-01-20138RMW), discussed in *‘Digital Wars And Fair Use,’ Federally Speaking*, No.23, as stated therein, “Adobe, the producer of the subject ‘e-books’ ... handed the **FBI** the case on a ‘cyber-platter’.” According to the affidavit in this **Federal Criminal Prosecution** of **FBI** Special Agent Daniel J. O’Connell, assigned to the **FBI’s High Tech Squad** at San Jose, California, “Adobe purchased a copy of the ElcomSoft unlocking software over the Internet ... Thereafter, ElcomSoft ... electronically sent the unlocking key registration code from ElcomSoft [in Russia] to the purchaser (Adobe) in San Jose, California ... A review [by Adobe] of the opening screen on the ElcomSoft software purchased showed that a person named Dmitry Sklyarov is identified as being the copyright holder” of this AEBPR unlocking software. “Adobe learned that Dmitry Sklyarov is slated to speak on July 15, 1001 [sic: 2001] at a conference entitled Defcon-9 at Las Vegas Nevada” and advised me that “Sklyarov is scheduled to make a presentation related to the AEBPR software program” there. The **Government** arrested and indicted Sklyarov when he visited the U.S. for this conference. From Adobe’s viewpoint, a great result. Adobe was able to drop its civil lawsuit and let the **Government** proceed criminally in its stead. (For another viewpoint, see **Digital Wars, supra.**) Thus, the bottom line of this “Heads Up” for plaintiff counseling is “it may be worth a shot to seek **Fed** involvement, if available it could be cheaper, harsher and more effective.” However, the “Heads Up” bottom line for defense counseling is more ominous: “**Fed** bullets may be a flying, keep you bottoms low and heads down!”

**THE FTC AND CONSUMER PRIVACY.** Subsequent to the terrorist activities of September 11, 2001, **Federal Trade Commission** Chairman Timothy J. Muris outlined the **FTC's** new and continuing Privacy Agenda, which includes increasing resources dedicated to consumer privacy protection by 50 percent. He pledged that the **FTC** “will do all it can to protect consumer privacy in the commercial realm - both online and off-line.” According to Chairman Muris, the new Privacy Agenda will contain the following major law enforcement and education initiatives: Enforcing the Telemarketing Sales Rule and Protecting Consumers From Unwanted Telemarketing; Creating a National Do-Not-Call List; Regulating and Restricting the Use of Pre-Acquired Credit Card Numbers and Account Information; Prosecuting and Stopping Pretexting, which is Outlawed by the **Gramm-Leach-Bliley Act (GLB)** (“pretexting” is the practice of obtaining personal financial information by fraud); Beefing Up Enforcement Against Deceptive Online Spam; Enforcing The **Children's Online Privacy Protection Act** (to prevent the collection of personally identifiable information from young children without their parents' consent); Controlling Identity Theft and Helping Victims of ID Theft; Encouraging Accuracy in Credit Reporting and Increasing **Fair Credit Reporting Act (FCRA)** Enforcement (the nation's first major privacy protection law); Enforcing Private Privacy Policies and Promises; Tracking and Improving Consumers' Privacy Complaint Handling; and Holding Privacy-related **FTC** Workshops. Indeed, since the provisions of the **Gramm-Leach-Bliley Act**, outlawing "pretexting," went into effect in 1999, the **FTC** has already increased its enforcement efforts to stop the misuse of sensitive financial information, and has recently obtained injunctions against information brokers in three different cities, using evidence obtained through a telephone sting operation. Muris advised that the **FTC** “will expand our activities here to examine other practices that try to obtain personal information through misrepresentations.”

**"Operation Cyber Loss."** "Operation Cyber Loss" is the code name for a nationwide series of investigations into Internet fraud initiated by the **Internet Fraud Complaint Center (IFCC)**, the first partnership between a federal law enforcement agency (the **FBI**), and a non-profit private organization (**the National White Collar Crime Center** or "NW3C"), which serves Federal, state and local law enforcement agencies. So far, the fraud schemes exposed by this Operation effected over 56,000 victims who suffered cumulative losses in excess of \$117 million, and include multi-level marketing and Ponzi/Pyramid schemes and schemes involving on-line auction fraud, systemic non-delivery of merchandise purchased over the Internet, credit/debit card fraud, bank fraud, and investment fraud. For victims of Internet fraud, the **IFCC** provides a convenient and easy way to alert authorities to suspected criminal or civil violations through the **IFCC** web site at [www.ifccfbi.gov](http://www.ifccfbi.gov). "Just as neighborhood watch programs keep watch over their neighborhoods and report suspicious activity to law enforcement, Internet users now have a cyber community watch," remarked **US Attorney General Ashcroft**. Most recently, Federal and state **fraud by wire, mail fraud, bank fraud, money laundering, and intellectual property right violations** criminal charges have been filed. To date Operation Cyber Loss has been participated in by **28 FBI Field Offices**, the **U.S. Postal Inspectors Service**; the **Internal Revenue Service-Criminal Investigative Division**; the **Securities and Exchange Commission**; **U.S. Customs Service**; the **Competition Bureau in Canada**; and numerous state and local law enforcement agencies.

**ALERT! CARNIVORE RUNNING RAMPANT!** According to an ACLU Alert, the **Federal Bureau of Investigations (FBI)** is ignoring the privacy protections of the **Fourth Amendment** and sinking its teeth into the Internet by conducting searches on the Internet through the use of an online wiretapping system labeled "**Carnivore**." The **FBI** allegedly "forces Internet Service Providers (ISP's) to attach a black box to their networks -- essentially a powerful computer running specialized software - through which all of their subscribers' communications flow." In traditional wiretaps, the government is required to "minimize its interception of non-incriminating -- or innocent -- communications. But Carnivore does just the opposite by scanning through tens of millions of emails and other communications from innocent Internet users as well as the targeted suspect." It is reported that Rep. Richard Arney (R-TX) has recently announced that he is considering seeking "budget cuts" to stop the **FBI's** use of Carnivore.

**CARNIVORE AND THE USA PATRIOT ACT.** Under the "**USA Patriot Act**," a/k/a the Anti-Terrorism Legislation (and also "an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"), ... in addition to the more "draconian" provisions "sunsetting" in four years, the Attorney General's power to detain/incarcerate non-citizens based on mere suspicion is limited to seven days (if deportation proceedings have NOT been commenced); the use of "Carnivore" devices, which scan "through tens of millions of emails and other communications from innocent Internet users as well as the targeted suspect," as reported on in the October 5, 2001 **Federally Speaking** column, is regulated by excluding general access to the "content" of the messages and by requiring Carnivore Reports to **Congress**; and the **Inspector General** of the **U.S. Department of Justice (DOJ)** is required to designate an official who shall review information and receive complaints alleging abuses of civil rights and civil liberties by employees and officials of the **DOJ**, publicize the responsibilities and functions of and how to contact this official, and semi-annually submit Reports to **Congress** on the implementation of this requirement and the details of the abuse complaints received.

**MAGIC LANTERN 21<sup>ST</sup> CENTURY-STYLE.** When we think of a "Magic Lantern" we envision a primitive "moving" picture device or, perhaps, Aladdin rubbing his Genie generator. No longer. In the 21<sup>st</sup> Century "Magic Lantern" will now refer to a "Trojan Horse" type computer program. According to **PC World**, Magic Lantern is being developed by the **FBI** to be planted by an agent "in a specific computer by using a virus-like program." Once planted, this keystroke logger "will render encryption useless on a suspect's computer" by capturing "words and numbers as a subject types them (before encryption kicks in), and will transmit them back to the agent." According to **FBI** spokesperson Paul Bresson: "It's no secret that criminals and terrorists are exploiting technology to further crime. The **FBI** is not asking for any more than

to continue to have the ability to conduct lawful intercepts of criminals and terrorists." Jim Dempsey, Deputy Director of the **Center for Democracy and Technology**, is concerned about the lack of prior notice of such "searches and seizures" as required by the **Fourth Amendment** to the **U.S. Constitution**: "In order for the government to seize your diary or read your letters," Dempsey advises, "they have to knock on your door with a search warrant," but Magic Lantern "would allow them to seize these without notice. ... The program would not only capture messages you sent, it would capture messages that you wrote but never sent." The main concern here appears not to be the use of new technologies, but the apparent lack of appropriate **judicial supervision**. Previously, **Federally Speaking** has reported on the use by agencies such as the **FBI** of "Carnivore" devices, which scan "through tens of millions of e-mails and other communications from innocent Internet users as well as the targeted suspect" (October 5, 2001 column), and how the **Patriot Act** tries to regulate their use "by excluding general access to the 'content' of the messages and by requiring Carnivore Reports to **Congress**" (December 14, 2001 column).

**LIBRARIES, THE INTERNET AND FREE SPEECH.** The third **Congressional** attempt to censor the Internet is now before a Three-Judge **U.S. District Court Panel** in Philadelphia, headed by Chief Judge Edward R. Becker of the **U.S. Court of Appeals for the Third Circuit**. Also on the panel are U.S. District Judges Harvey Bartle, III and John P. Fullam. An appeal from this panel will go directly to the **U.S. Supreme Court**. Under attack this time is the **Children's Internet Protection Act of 2000 (CIPA)**, the federal law that requires libraries to install Internet filtering software in order to receive **Federal** technology funding to provide library users with Internet access. The **Communications Decency Act of 1996**, **Congress's** first attempt to control pornography on the Internet, was thrown out by the **U.S. Supreme Court** as being an **unconstitutional** infringement of **free speech**. The enforcement of **Congress's** second attempt, the **Child Online Protection Act of 1998**, has been enjoined pending the decision of **U.S. Supreme Court**, which is expected later this year. Both the 1996 and 1998 **Acts** imposed criminal penalties. A coalition of libraries, library users, Web site operators and the American Civil Liberties Union is seeking a permanent injunction against this latest attempt at censorship, as a violation of **free speech rights**. Additionally, the **CIPA** is under attack as imposing costly monetary burdens on libraries that are forced to comply or lose funding. Proponents of the **CIPA** believe that as this legislation only withholds funding and does not impose criminal sanctions, and as it permits adults to ask for the filtering software to be turned off for "bona fide research" reasons, it is the "**government's** best shot yet" at controlling Internet access without being held to be in violation of the **free speech** guarantees of the **First Amendment to the U.S. Constitution**. Conversely, opponents believe that these threats of withholding funding, and the embarrassing necessity of having to ask, and of having to give a "bona fide" reason, to have these filters turned off, have **unconstitutional** "chilling" affects on **free speech**. Whatever the outcome, we know that the "price" for **free speech** is constant vigilance.

**INTERNET CENSORSHIP – PAGE Three.** Page Three, **Congress's** third attempt to censor the Internet has now unanimously failed before a Three-Judge **U.S. District Court Panel** in Philadelphia, in an opinion written by Chief Judge Edward R. Becker of the **U.S. Court of Appeals for the Third Circuit**, and joined by **U.S. District Court** Judges Harvey Bartle, III and John P. Fullam. An appeal from this panel goes directly to the **U.S. Supreme Court**. As originally reported in the May, 2002 issue of **Federally Speaking**, the **Children's Internet Protection Act of 2000 (CIPA)** required "libraries to install Internet filtering software in order to receive **Federal** technology funding to provide library users with Internet access." The **Three-Judge Panel**, in issuing a **permanent injunction**, found that: "As our extensive findings of fact reflect, the plaintiffs demonstrated that thousands of Web pages containing protected speech are wrongly blocked by the four leading filtering programs, and these pages represent only a fraction of Web pages wrongly blocked by the programs.... In view of the limitations inherent in the filtering technology mandated by **CIPA**, any public library that adheres to **CIPA's** conditions will necessarily restrict patrons' access to a substantial amount of protected speech, in violation of the **First Amendment**" (see the consolidated cases of *Multnomah County Library vs. U.S.*, No. 01-CV-1322, and *American Library Association vs. U.S.*, No. 01-CV-1303 (EDPA, 2002)). Page One was the **Communications Decency Act of 1996**, **Congress's** first

attempt to control pornography on the Internet, which was thrown out by the **U.S. Supreme Court** as being an **unconstitutional** infringement of **free speech**. The enforcement of Page Two, **Congress's** second attempt, the **Child Online Protection Act of 1998**, has been enjoined pending the decision of **U.S. Supreme Court**, which is still expected later this year. For more on the "Wars Against Pornography and Free Speech," and a possible "Page Four," see "Operation Candyman," above.

**OPERATION CANDYMAN.** We first learned about the "Candyman" in 1971 from "Willy Wonka and the Chocolate Factory," as a purveyor of "goodies to children." Well, the **U.S. Department of Justice** recently appropriated the "Candyman" and converted him into an "Operation" to deter purveyors of "children as goodies," by focusing in on the alleged illegal activities of Internet "child-pornography" chat groups. "A new marketplace for child pornography has opened in the dark corners of cyberspace," but there "will be no free rides on the Internet for those who traffic in child pornography," announced **U.S. Attorney General** John Ashcroft. Hitching on to this Candy Wagon, Alan Sekulow, the ACLJ's Chief Counsel and self-styled opponent of "threats to Christian freedom," now asserts that "**Operation Candyman**" unmistakably shows the need for the enactment of the new **Child Obscenity and Pornography Protection Act of 2002**, "that would make the depiction of children - virtual or real - engaging in sexual acts **ILLEGAL**," and solicits support from his followers "because of the **Supreme Court's** decision this spring" overturning the **Child Pornography Prevention Act of 1996 (CPPA)**, which, according to Counselor Sekulow, "effectively **LEGALIZE CHILD PORNOGRAPHY**" (*Ashcroft v. The Free Speech Coalition*, No. 00-795 (Sup. Ct. 2002)), and "because the ACLU and other organizations are lobbying in Washington to protect the so-called '**free speech rights**' of pornographers" (**CAPITALIZED** emphasis **NOT** added). The **CPPA** had tried to ban a wide variety of artistic techniques, including the use of child-like adults and computer created pictures, to portray the appearance of explicit youthful sexuality (including "a la Romeo and Juliet"). Justice Anthony Kennedy, writing for the 6-3 majority, found that the main provisions of the **CPPA** were "overbroad," thus violating the **First Amendment** guarantee of **Freedom of Speech**. Ironically, Mr. Sekulow, the **FBI** advises that the **Government** in proceeding with its **Operation Candyman** prosecutions *under present law* has so far netted at least eight members of the clergy, including two Catholic priests (and a law enforcement employee). The more relevant questions, therefore, appear to be: "Whose houses really need cleaning?" and "Do we really need more legislation that very well will not survive **Constitutional** muster, or just proper enforcement of existing laws? (Interestingly, the same latter question is being asked with regard to our "War Against Terrorism.") For more on the "Wars Against Pornography and Free Speech," see "Internet Censorship – Page Three," below.

**"RESISTANCE IS NOT FEUDAL."** So scribed Jim Girard in a recent Lockergnome e-mail column. He was cautioning against the "**Security Systems Standards and Certification Act**" (**SSSCA**), a proposed, apparently "Borgian," entertainment industry Bill which would require all new personal computers to have built-in "**policeware**" to prevent apparently even "fair use" copying of **Copyrighted** materials, and which would carry with it **Federal Criminal Penalties** of up to five years in **Federal Prison** and \$500,000 in fines, for disabling or tampering with such "**policeware**." Why "Feudal"? Because according to the self-ascribed "scribbles" of this Scribe, if this Bill were to become law "it would represent the first such restriction on the individual use of intellectual property (at least in a Western democracy) since the Middle Ages," where "resistance was futile," for, as he advised, the Medieval Church "controlled what was read and who got to read it. All books were held in church libraries and copied only by monks, and it was necessary to take religious orders even to learn how to read. ...The invention of moveable type made it possible for writers and readers to bypass the Church's control of information, and communicate with one another directly," sparking, he asserted, the "Renaissance" and the "Reformation." Scribe Jim views the **SSSCA** as an "**unconstitutional**" and, hopefully futile, return to Freudianism, oops! Feudalism, and directs all Anti-Borgians to go to "StopPoliceware.com" to "Join the Resistance" (<http://www.stoppoliceware.com/>)

**Free You Say ... ?** "These so-called 'free' Internet access offers" by Juno and Gateway "were anything but," advised Jodie Bernstein, **FTC Bureau of Consumer Protection** Director. Juno made it most difficult, the **FTC** charged, for surfers to cancel their "free" Internet premium service trial period by only allowing cancellations through one telephone number, which, you guessed it, was kept unpublished, and when they finally reached this number they were, of course, kept waiting for long periods of time. Juno was also charged with failing to adequately disclose that surfers might incur long-distance telephone charges while on the Web; hiding information about fees "in the fine print;" not adequately disclosing that the 150 free hours had to be used within a month; and starting the one-month free period before the software necessary to access Juno was received. Similarly, the purchasers of Gateway Essential Computers were allegedly rewarded with free "Gateway.net" Internet access for one year. However, those who could not access Gateway through local phone numbers were actually charged \$3.95 per hour for use of "essential" so-called "toll-free" connections to "Gateway.net". The five **FTC** Commissioners unanimously voted for consent agreements with these companies which, among other things, will prohibit them from "misrepresenting the price or cost of any service to access the Internet or other electronic network," and will require the payment of refunds to consumers.

**THE FREE INTERNET CONNECT CON.** For half a year we have been exposing hidden charge scams and cons and have been trying to invoke the help of the "**Old Lady on Pennsylvania Avenue**" (the "**FTC**"). Along the way we were happy to learn that a Consumers Union study has reached similar conclusions to ours, to wit, that there exists "prevalent pervasive practices of sellers adding extraordinary and unexpected charges, many of them disguised and/or hidden, to consumer products and services." Our latest exposé is the free Internet connect con. "FreeInternetConnection.com" (FIC), as its name clearly states, brings you to its web page through the promise of a "free internet connection," for which you would actually "pay" through your receipt of banner advertising as part of this "free" connection. But here, as you will see, you will also "pay" in additional ways. Upon arriving there you are first informed that you **must** apply for and be granted an American Express, MasterCard or Visa credit card, or as suggested, why not apply for several? After successfully applying, you may be told that the connect service is temporarily down or the way may then be opened for you to the next surprise, that is that only after applying, being accepted and proceeding through a number of screens, do you learn that there is a hidden "\$19.95 setup fee" for this so called "free internet connection." And when confronted with this deceit, what does FIC then have to say? "**Yes** there is a one time set up charge, *however this is not uncommon in this and many other facets of the internet services industry whether initially divulged or not [shades of Federal Sherman Antitrust Act conspiracies]*. ... You are under no obligation to sign up for the free Internet service and/or to keep the card you applied for" (emphasis added). But what obligations are FIC under? Least you do not believe FIC that this "**is not uncommon**," you need only respond to the tempting offer, as proclaimed from billboards, by "PghConnect.com," of a months internet access for only \$6.95. As nowadays most surfers expect paid connections to be without time limits, the first surprise occurs when you are stopped cold at the screen advising only "30 hours monthly service included" (or only one hour a day). But what we are concerned about here this month is being informed several screens later that: "Monthly accounts will be charged a one-time \$5.00 setup fee." See also "Access995.com" with unlimited monthly access at \$9.95 and such a setup fee of \$29.95, and "Libcom.com" with unlimited monthly access also at \$9.95 and such a setup fee of \$19.95. If you would like to add your voice with regard to these or any other hidden, unexpected or extraordinary charges, the **FTC** file reference is "**FTC Ref. No. 1787101**," and tell us also so we can consider your uncovered scam or con for further exposure in this column.

**An "E-Sign of the Times"** – Imagine creating a brilliant original lead, only to find, upon surfing the Web, that it had already been previously "e-stolen" (well almost, not the "an"). Certainly, an "e-sign of the times." Another "e-sign of the times" is the **Electronic Signatures in Global and National Commerce Act of 2000** or the **E-Sign Act**. According to an article electronically published under the title E-Sign of the Times, by Wittiel & Winn (Kirkpatrick & Lockhart Web page, <http://www.kl.com/PracticeAreas/Technology/pubs/page20.stm>), the **E-Sign Act** "will reduce the

uncertainty surrounding the use of electronic media in transactions and permit more businesses to realize the cost savings possible with electronic commerce,” for the “Act effectively sweeps away a myriad of anachronistic and inconsistent state and federal law requirements for paper and ink documents and signatures, and permits electronic commerce to proceed on a substantially uniform legal basis nationwide.” It prohibits the denial of enforceability, validity or legal effect to a contract based solely on it having an “electronic signature” or being in electronic form. But as Ervin, Cohen & Jessup of Beverly Hills cautions, “the exchange of cursory e-mails between a supplier and customer – ‘I think \$1000 per unit.’ ‘Sounds good.’ – could create a binding contract,” both in and/or between Beverly Hills and the North Hills.

**THE FAX, JUST THE FAX, MA’AM!** The Federal Communications Commission (FCC) is on the offensive against “broadcasters” who send, to private facsimile machines, hundreds of thousands of unsolicited “junk” advertisements each day. Enforcement action is being sought under the **Telephone Consumer Protection Act of 1991**, which provides that: “No person may transmit an advertisement describing the commercial availability or quality of any property, goods or services to fax machine without express permission or invitation.” John Winston, the assistant chief of the **FCC Enforcement Bureau**, reported that the number of formal consumer complaints about junk faxes has grown from approximately 300 in 1997 to more than 1,400 last year. We are advised, that under current Federal law, in addition to **FCC** fines, consumers can seek from broadcasters of junk faxes, in state court, up to \$1,500 for each violation, and do so as Class Actions.

**SEE YOU NEXT YEAR IN THE COURTROOM OF THE FUTURE!** The Federal Bar Association, West Penn Chapter, on behalf of the **U.S. District Court for the Western District of Pennsylvania**, again provided instruction to the local **Federal Bar** on the awe and wonder of the new **Electronic Courtroom**, through its well-received and fully subscribed CLE program “The Ons and Offs of The Electronic Courtroom.” This year the off-site witness, who was the subject of direct and cross-examination, testified from Chicago. In the absence of Judge Cindrich, yours truly presided, adding “redaction” to the bag of electronic tricks. The next session will be held in a year. Check this column for date and time. The place, as always, will be the **Federal Courthouse**, in the **Electronic Courtroom** presided over by **U.S. District Judge Robert J. Cindrich**

**BACK ISSUES.** This column often carries stories continuous in nature, and may “bring issues back” or even “back into issues.” To aid in getting the “whole story,” the **U.S. District Court for the Western District of Pennsylvania** has graciously made all back issues of *Federally Speaking* available on their web site at <http://www.pawd.uscourts.gov/Headings/federallyspeaking.htm>.

\*\*\*

*The purpose of **Federally Speaking** is to keep you abreast of what is happening on the Federal scene Please send any comments and suggestions you may have, and/or requests for information on the Federal Bar Association to: Barry J. Lipson, Esq., FBA Third Circuit Vice President, at the Law Firm of Weisman Goldman Bowen & Gross, 420 Grant Building, Pittsburgh, Pennsylvania 15219-2266. (412/566-2520; FAX 412/566-1088; E-Mail [blipson@wgbglaw.com](mailto:blipson@wgbglaw.com)).*

Copyright© 2003 by the Federal Bar Association, Western Pennsylvania Chapter.