

PRACTICING LAW IN CYBERSPACE

By Al Harrison
Harrison & Egbert
VirtuAl@hypercon.com

Federal Bar Association
January 20, 2000

Introduction

Having the ability to practice law in Cyberspace has virtually metamorphosed the legal landscape into an amorphous mass. This amorphous mass is actually populated with an underlying structure of well-established legal principles and practices blanketed with a colloidal covering. Besides compelling changes in the manner in which legal services are delivered, this has introduced a plethora of ethical concerns for lawyers and law firms.

Consider the following questions: With whom are you communicating by sending email? Are you inadvertently providing legal advice to an unknown person in an unknown venue? For free? Have you inadvertently established an attorney-client relationship? Are you licensed in the state in which the recipient resides? Do you routinely check all incoming data for viruses? Do you exercise diligence safeguarding your firm and client information stored on your network? Is encryption prerequisite for safeguarding such information? Passwords? Biometrics?

Venturing into Cyberspace is easy to effectuate: one simply need be positioned proximal to a keyboard and pointer device, and then interact with the operating system and application (browser or email or news-reader or chat) software. Nevertheless, as members of the legal profession are rapidly discovering, this ease of entry has the potential to drastically affect peace of mind and integrity of practice.

“E” Whatever

The Internet continues to permeate modern life as we know it as a diversity of activities and transactions migrate into Cyberspace. The prefix “e” is becoming a standard preface for virtually everything. For what does this conspicuous “e” (or is it “E”) stand? Electronic? Extraordinary? Erratic? Emerging? Emergency? Extraneous? Extemporaneous? Ephemeral? Whatever “e” applies in a particular circumstance, the information will be disseminated via a distribution system that is virtually infinite in geographical scope — and that traverses time barriers.

Email, of course, may be forwarded at the sender’s convenience and whim. Similarly, email may be read at the recipient’s convenience and whim. Indeed, a(n) incipient recipient may elect not to read an incoming email, and delete it. If an email is accompanied by one or more attached files, a recipient has the option to open this file and then read it. Computer viruses may, unfortunately, be present

in an attached file. Viral behavior may be propagated by merely receiving an email. Similarly, viruses may be introduced via downloads from Web sites or during chat sessions. Some of the newer varieties of electronic infections behave unpredictably, perhaps more like a flu-like condition than a virus.

A computer virus is essentially a prevalent form of electronic terrorism that may alter the normal operation of computer programs, modify or destroy data, and potentially eradicate the contents of a hard disk. In the context of the Internet or corporate intranets, virus are particularly dangerous because its Cyberscape provides an inherently fertile landscape for rapidly propagating any form of electronic invasion.

A computer virus is a malicious self-replicating computer program that infects a target or host file by attaching thereto. Generally, by thus attaching to an executable file, driver, or document template, such a virus adversely affects the behavior of the underlying application or operating system computer programs. Not unlike a viral infection of a human, a computer virus metamorphoses a normal executable file — a computer program that performs predefined functions — into a carrier of infection. Once this carrier file is executed, the virus may be replicated, typically without affording time for recovery procedures to be effectuated. Thus, akin to a communicable infection, propagation occurs when this virus encounters predisposed host sites: a computer virus is typically targeted to strike an executable program such as Microsoft Word, a driver such as a driver for a particular hardware device, or a document format such as a Microsoft Word or Excel file. Viruses are typically introduced onto a host site via a file copied from a diskette or downloaded from the Internet.

The modus operandi for invasion by a computer virus is to, first, infect memory when the host file is invoked by the operating system (in response to a user's command), and, then, to intercept and infect all subsequent applications or the like that are invoked. Systemic infection of a computer or network typically results. A "worm" is a particularly dastardly variation of a virus that is designed to infect a target network by first attaching itself to a host computer and then spreading to other host computers throughout the network, typically simultaneously undermining network resources.

There are several types of computer virus, including a boot sector virus, a macro virus, an overwriting virus, and a multipartite virus. A boot sector virus infects the boot sector of a diskette or a hard disk and then propagates itself onto every diskette placed into the diskette drive. A macro virus is typically propagated

when a Microsoft Word file is attached to an e-mail message. An overwriting virus, as its name implies, simply overwrites each file that it infects, thereby rendering the infected file inoperable. A multipartite virus infects multiple aspects of a computer and file types. For example, a multipartite virus may infect a computer's boot record and also executable application files. As another example, a multipartite virus may infect device drivers (for a mouse, or a printer, etc.) and executable files.

Two common attributes of computer virus are "stealth" and "polymorphic" behavior. A stealthy virus conceals a file being infected generally by saving and then feeding back to the user pre-infection information. That is, a stealthy virus pretends that all is well by ostensibly generating normal feedback messages and the like to users. A polymorphic virus, on the other hand, exhibits schizophrenic behavior in the sense that it eludes detection by varying its underlying (byte-oriented) personality. Accordingly, advanced scanning detection techniques are prerequisite to diagnosing viral patterns so that a suitable antidote may be used to neutralize the polymorphic virus.

To prevent viral invasion of computer and computer networks, all incoming files — locally, via removable input devices such as conventional 3½" diskettes, SuperDisks, and zip disks, or remotely, via e-mail attachments or Internet downloads — should be routinely checked for the presence of viruses. If a virus is found on a storage medium, besides this medium being inoculated, the source of the virus should be investigated and noted (to avoid future recurrences) and reported as appropriate. Anti-virus software should become standard operating equipment to regularly scan and thereby monitor all system activity (unobtrusively in the background) to assure early virus detection. Functioning as virtual device drivers, anti-virus software checks everything that penetrates a computer's territory including every input peripheral device accessing a file and every application that is run.

This specialty software ideally has the benefit of the most current knowledge of all existing computer viruses, and uses advanced detection techniques incorporating sophisticated algorithms, stochastic analysis, and heuristics. Inexpensive superior anti-virus software applications are provided by Symantec Norton, Network Associates' Dr. Solomons and McAfee, and Mijenix SystemSuite. Generally, it is imperative to keep this software in synch with the state of the art, i.e., currently known viruses, by subscribing to the vendor's online update and maintenance services — including a virus alert service.

Gate-keeping tools such as “firewalls” should preferably be used at entry points into intranets to further secure network environments. A firewall typically prevents the incursion of external communications through its wall-like barrier unless the computer user requested this communication. For example, firewall software would permit the entry of data corresponding to a Web page in response to a browser requesting that the Web page be downloaded for viewing. Nevertheless, other gate-keeping tools are becoming essential.

Electronic terrorists have discovered another dastardly *modus operandi* for conducting e-invasions primarily via a Trojan horse. A tainted application parked on your hard disk may access the Internet without your authority or knowledge. When a channel to the Net has been opened to e-traffic, there is obviously a risk that nefarious hackers and the like can seek to achieve oneness with your computer. Preventing such unauthorized information flow from your computer may be achieved by using blocker software such as ZoneLabs’ ZoneAlarm (www.zonlabs.com). Email may be screened (without implicating attached files) before being actually downloaded to your hard disk via software such as Email Remover (eremover.bizhosting.com). Thus, before an email is read *in toto* or an attached file is downloaded, only the “headers” or only a portion of the message may be screened to ascertain whether its Kosher.

URL-Invasion of Trademark Domain

Assignment of URLs as locators for finding Web sites has caused and will continue to cause tension with well-established principles of trademark law. Originally intended to simply provide a “street address” for a Web site, a URL — consisting of a string of low-to-high domains, collectively referred to as a “domain name” — are frequently selected for trademark purposes. This is to primarily identify the source of origin of the site. Hence, a Web surfer entertaining a visit to the Web site located at “www.compaq.com” would expect to have a nexus with products and services of Compaq Computer. Similarly, a visitor to the site “www.movebuff.com” would anticipate enjoying the services associated with the well-known The Movie Buff’s Movie Store.

Interestingly, this was the theory of Brookfield Communications, Inc. based upon its registered “moviebuff” trademark until West Coast Entertainment Corp. obtained the URL for www.movebuff.com. Brookfield sought and was granted injunctive relief alleging trademark infringement and unfair competition under Sections 32 and 43 (a) of the Lanham Act, 15 U.S.C.A. §§ 1114, 1125 (a)(1), when the Ninth Circuit reversed the trial court’s judgment. 174 F.3d 1036, 50 U.S.P.Q. (BNA)

1545 (9th Cir. 1999). The trial court construed the ministerial process of acquiring a domain from a URL Registrar coupled with the intention to use the domain name for commercial purposes as establishing trademark rights. The Ninth Circuit properly rejected this misapprehension of establishing priority of use of a trademark in commerce and analogized West Coast's early uses to an address on a letterhead and to a legend on an architectural drawing.

Another significant development in Cyberspace is the prevalence of the phenomenon affectionately referred to as "Cybersquatting." Cybersquatting occurs when a URL containing an otherwise trademarked word or term is obtained by someone other than the trademark owner. While this activity may be inadvertent and innocent, Cybersquatting is usually performed for the purposes of selling the domain name to its "rightful" owner. Several domain names have, indeed, been sold for hundreds of thousands and even millions of dollars. Several lawsuits have been filed by trademark owners on the basis of likelihood of confusion and/or dilution theories. Now armed with the weapons of the recently enacted Anticybersquatting Consumer Protection Act, such suits are apt to propagate at least until this behavior subsides.

The Anticybersquatting Statute amends the Lanham Act to attribute civil liability to a person who has a bad faith intent to profit from another's trademark by registers, traffics in, or uses a domain that is distinctive or famous. A cybersquatter will be minimally required to forfeit or cancel or transfer the domain name to the owner of the underlying trademark. Several defensive factors are enumerated for determining whether the prerequisite bad faith occurred. A subtle aspect of this law is that domain name registrars will not be found to be liable for injunctive or monetary relief unless bad faith or reckless disregard was exhibited.

Did "Y2K" Happen Yet?

There is a prevalent attitude that Y2K was a non-event. Presumably the worst is over, but is it really over? For example, since 2000 is a super leap year, there will be 29 days in February. Will computer systems recognize this? We'll see. To keep abreast of Y2K activities, link to Carnegie Mellon University's Software Engineering Institute's CERT Coordination Center ("www.cert.org").

Many plaintiffs' lawyers are anxiously awaiting the floodgates to open against software vendors, computer hardware manufacturers, medical equipment manufacturers, and insurance companies. Y2K litigation has already commenced throughout the country. See, e.g., *Against Gravity Apparel Inc. v. Quarterdeck Corp.*,

No. 603752/98 (NY Sup.Ct., NYC 4/5/1999) (class action alleging that ProComm Plus telecommunications software knowingly marketed with Y2K defect and breaching express performance warranty dismissed because 90-day warranty period had expired); *Paragon Networks Int'l v. Macola, Inc.*, No. 9-99-2 (OH Ct. App., 3d App. Dist., Marion Cty., 4/28/1999) (dismissal of Y2K breach of warranty suit affirmed because underlying license recited a warranty disclaimer, a 90-day limited warranty, and an integration clause); *Mineral Area Osteopathic Hospital Inc., Community Memorial Healthcare Inc., and North Country Hospital, Inc. v. Keane, Inc.*, (N.D. IA, Cedar Rapids Div., complaint filed 3/21/1999) (class action alleging that Keane is "sunsetting" the non-Y2K compliant Mednet computer system by advising customers that maintenance and support would be discontinued unless user-hospitals waived all Y2K claims); *Vernis & Bowling of Miami, et al. v. Nortel Networks, Inc.*, No. 99-10186 CA 04 (FL Cir.Ct., 11th Jud.Cir., Miami-Dade Cty., complaint filed 4/26/1999) (class action alleging breach of warranty and unfair trade practices for selling non-Y2K compliant products that must be upgraded); *Johnson v. Circuit City Stores, Inc., Fry's Electronics, Inc., CompUSA Inc., Office Depot, Inc., OfficeMax, Inc.*, No. C99-00054 (CA Sup.Ct., Contra Costa Cty., 4/20/1999) (attempt to dismiss suit on the basis of failure to disclose whether products were Y2K-compliant because products are functioning properly now, i.e., prior to Y2K, denied); *Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc.*, No. 98-1084 (W.D. Pa 5/3/1999) (pursuant to plaintiff seeking class action status, defendant must answer written interrogatories pertaining to its licensing of non-Y2K compliant Synchronics cash register, inventory, and accounting software when its comparable Counterpoint Y2K-compliant software was commercially available; but defendant need not provide access to its technical personnel or to 3rd-party remediation software because of undue burden and violation of software license); *Rhodes v. Omega Research, Inc.*, No. 98 -0174-CIV-LENARD (S.D. Fl. 3/1/1999) (shareholder derivative action alleging that Omega and IPO underwriters failed to lack of Y2K compliance dismissed because prospectus disclosed high degree of risk). Settlement of class action litigation brought against Sage U.S., Inc. relating to the Y2K compliance of DacEasy and Timeslips software has been granted preliminary approval by the 44th District Court of Dallas County¹. A potentially significant complaint for declaratory relief has been filed by GTE Corporation against several insurance companies for indemnification for costs incurred to avoid or minimize loss associated with the Y2K problem.² Standard language recited in the various insurance policies indicates that the insurance company "insures against all risks of physical loss of or damage to property described therein," including "any destruction, distortion or corruption of any computer data, coding, program or software..." *GTE Corp. v. Allendale Mutual Insurance Co.*,

Affiliated FM Insurance Co., Allianz Insurance Co., Federal Insurance Co., Industrial Risk Insurers (D.N.J. filed 6/18/1999).

Of course, the maze of federal and state Y2K Statutes will be attempting to moderate the spate of lawsuits that have been and that will be filed throughout the year. The Y2K Act, signed by President Clinton on July 20, 1999, purports to provide incentives for businesses and individuals to engage in remedial activities, to seek to mitigate incipient and potential damages, and to test Y2K solutions, presumably before Y2K problems develop. The "Y2K Act," the short title for Pub. L. 106-37, strives to encourage businesses to approach Y2K disputes "responsibly" and expeditiously by engaging in good faith informal negotiations and ADR, thereby avoiding disruption to interstate commerce and burdening the courts with a deluge of "insubstantial" lawsuits and thus reserving the courts for lawsuits involving legitimate damage claims. To meet these goals, the Y2K Act attempts to broadly define a "Y2K Failure" in the context of "year-2000 date-related data" that manifests a failure of accurately processing "transitions or comparisons from, into, and between the years 1999 and 2000"; or of accurately processing "any date in either of the years 1999, 2000, or 2001"; or of accurately processing Y2K leap year specific date data, e.g., "including the recognition and processing of the correct date on February 29, 2000."

Texas, on May 21, 1999, enacted a Y2K Statute that is effective September 1, 1999 and applicable to lawsuits filed thereafter. S.B. 598. The Texas Y2K Statute is embodied in Title 6, Civil Practice and Remedies Code, Chapter 147, entitled "Year 2000 Computer Date Failure." With objectives similar to the Y2K Act, this statute recites a severalfold purpose: to protect and promote the well-being of the citizens, the health of the state economy, and the ability of state and local government to provide services by avoiding or mitigating Y2K problems; to establish incentives for encouraging the computer industry to effect the early identification of Y2K problems, and then to develop and implement timely solutions and to resolve disputes via ADR; to avoid burdening the judicial system with a plethora of specious lawsuits; and to preserve the rights of citizens seeking redress for bodily injury and wrongful death.

The statute is applicable only to actions that seek to recovery damages or any other relief for harm causally related to either a computer date failure or by a failure to properly detect, disclose, prevent, report, correct, cure, or remediate a computer date failure. A key concept of "computer date failure" is defined as "the inability to correctly process, recognize, store, receive, transmit, or in any way use date data referring to the Y2K or affected by the transition between the years 1999

and 2000, or with years expressed in a 2-digit format. It applies to the resolution of Y2K lawsuits that do not implicate death or bodily injury, workers' compensation benefits under Texas Workers' Compensation Laws, or the enforcement of a written contract or contractual remedies for contract breach that specifically recites provisions for liability and damages involved in a computer date failure.