techLAW

the link between law and dot.commerce

A Publication of

FARRELL FRITZ, P C

Issue 2, Volume 1
Fall 2000

Electronic Signatures... The New Federal Law

By J. Kemp Hannon
khannon@farrellfritz.com

Simple as signing your name? As the bankers, brokers, agents and lawyers planning e-commerce for their businesses have discovered, an "electronic signature" is anything but simple. Under new Federal legislation, ultimately transactions using an electronic signature will be simpler, easier and more efficient than the system to which we are now accustomed.

We are referring to the Electronic Signatures in Global and National Commerce Act signed June 30th by President Clinton, effective October 1, 2000 (with various effective dates for specific provisions, such as the use of electronically transferable records under the UCC, or the SEC regulations for advertising or sales literature, or general record keeping).

We all think that we know what a "signature" is. That's exactly the legal system's problem when it comes to recognizing a signature. Under common law a signature is considered a subjective act . . . whatever a person did to be one's own signature is in fact one's signature. From novels of the Old West, where a person's "X" could be a signature, to the modern day, where members of a certain profession are derided for their infamous and undecipherable scrawl or "mark," verification of signatures is a continued legal challenge.

So too for commerce over the Internet. While radio, then TV, then phones and later faxes all had interesting aspects for doing business, the Internet allows for the complete delivery of complex information in a

continued on page 4

Linking to Illegal Software Generates Liability for the Linker

By Jonathan I. Ezor
jezor@farrellfritz.com

On August 17, 2000, Judge Lewis A. Kaplan of the Southern District of New York ruled in favor of Universal City Studios and seven other major motion picture studios in a case involving the publication of DeCSS, a program written to defeat the copy-protection found on DVD movies. The decision raises the possibility that linking to another Web site in certain circumstances may in itself generate legal liability for the linker. DeCSS was written last year by a then-sixteen year old Norwegian programmer named Jon Johansen and distributed over the Internet. While the program was ostensibly written to decrypt DVDs for display on computers running Linux, an operating system for which there are no current legal DVD players, the software also enabled users to copy and distribute movies over the Internet and (with some additional process) via CDs. The defendants in the

continued on page 6

Corporate Counsel Corner
Third Circuit Strikes Down Child Online Protection Act

By James M. Wicks
jwicks@farrellfritz.com

The Third Circuit Court of Appeals recently found constitutional infirmities in the Child Online Protection Act ("COPA"), 47 U.S.C. § 231, which prohibits knowingly communicating over the World Wide Web for commercial purposes material that is "harmful" to minors. COPA was enacted in October 1998 in response to the Supreme Court striking down the predecessor legislation, the Communication Decency Act, which was introduced in an

continued on page 2

INSIDE THIS ISSUE

FARRELL FRITZ, P C
EAB Plaza
Uniondale, NY 11556-0120
(516) 227-0700
www.farrellfritz.com

Bill Bans Secret Workplace Snooping

By Andrew L. Crabtree
acrabtree@farrellfritz.com

Still have no employee Internet use policy in place? . . . Well, a bill recently introduced in the U.S. Senate would make it illegal for companies to secretly monitor employee e-mails, Web use and telephone calls. Under the proposed "Notice of Electronic Monitoring Act", employers would be required to give notice to employees of all forms of electronic monitoring of e-mail, Web use or phone conversations. The proposal would amend the Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq*.). Although "snooping" wouldn't be banned, companies would now have to disclose their monitoring practices to newly hired employees and update all employees annually.

As the law now stands, an employer may monitor employee e-mail and Internet usage for valid business purposes. The risks are too high not to: harassing, racist or otherwise offensive messages or downloads could create a "hostile work environment"; copyright or criminal laws may be violated by sending proprietary or pornographic material; and unguarded e-mails may come back to haunt an employer in the midst of litigation.

Courts have generally upheld an employer's right to monitor e-mails, so long as the employees are put on adequate notice of the policy, so that the workers have little or no expectation of privacy in their e-mail or Internet use. Adopting a clear policy is essential. No employee handbook is complete without it. The written policy should make clear that, among other things:

- the e-mail system is company property;
- all e-messages are company records whose publication is prohibited;
- the company reserves the right to monitor all e-mail, telephone calls, and Internet usage without notice;
- e-mail is restricted to business purposes only;
- harassing, discriminatory or destructive (virus-type) messages or downloads are prohibited;
- disclosure of confidential, proprietary or copyrighted information is prohibited; and
- written employee consent is given.

Under the proposal sponsored by Sen. Charles E. Schumer, an employer who monitors any wire, oral or electronic communication (including telephone calls) may be held civilly liable to an employee, unless a clear and conspicuous notice describes:

- the form of communication or computer usage that will be monitored
- the methods of monitoring and the kinds of information that will be obtained; including whether non-business (i.e., personal) communications or computer usage will be monitored
- the frequency of such monitoring
- how the information obtained will be stored, used or disclosed.

Therefore, every company that seeks to monitor employee computer and telephone usage should ensure that its policy contains the above information as well. For a violation of the law, an employer would be subject to civil damages of up to $20,000 per employee; or $500,000 per incident, in cases in which many employees were affected, as well as punitive damages, court costs and attorneys' fees.

Notably, however, the bill would still allow employers to secretly monitor any employee if there is a "reasonable" suspicion that illegal activity is taking place and that electronic monitoring will produce evidence of that conduct.

While the bill may actually encourage employer monitoring of employee e-mail and Web use, it should certainly encourage all companies that permit employees to use e-mail and the Internet to protect itself with an adequate employee computer use policy.

The bill was introduced in the Senate on July 20, 2000 and sent to the Judiciary Committee on July 21, 2000. The Senate has taken no action since re-convening in September. We'll keep you informed.

Andrew L. Crabtree, an associate in the Commercial Litigation Department at Farrell Fritz, represents clients in state and federal courts and arbitrations with a growing emphasis on technology matters.

Child Online Protection Act Struck Down

continued from page 1

effort to regulate minor's access to web-based pornography.

In upholding the grant of a preliminary injunction, the Third Circuit held that the statute does not adequately address the Supreme Court's concerns over the definition of "contemporary community standards." The lack of geographic constraint over the reach of the Web - *i.e.*, a Website owner cannot prevent certain locales from accessing the site - renders the statute overbroad, since "contemporary community standards" in one locale may very well differ from another. Since a Website cannot distinguish the locale in which it is accessed, the definition is overbroad.

In finding COPA to be unconstitutional, the court made it clear that technology one day may render the concerns raised by the court moot. That is, the court recognized that although it is not technologically feasible today to geographically restrict the broadcast of a Website, that may not be the case in the future.

James M. Wicks, a partner in the Commercial Litigation department at Farrell Fritz, represents businesses, financial institutions and individuals in federal and state courts involving a variety of commercial, technology, real estate, and banking issues.

Issuers Acting Online: The SEC Speaks . . . Again

By Lyle C. Mahler
lmahler@farrellfritz.com

Since the U.S. Securities and Exchange Commission published its first release governing online activities of issuers of securities in October of 1995, the SEC has kept close watch over the activities of issuers acting online as technology has advanced.

Recently, the SEC published additional interpretive guidelines for issuers of securities who seek to contact investors and potential investors through the Web. The interpretations took effect on May 4, 2000, however the SEC invited comment on the new guidelines and several issues addressed in the release through June 19, 2000 in order to assess whether further regulatory action is needed.

To date, several comments have been submitted to the SEC, including comments from Fidelity Investments, the National Association of Bond Lawyers and the Florida Division of Bond Finance. Although it is too early to determine whether the SEC will act upon any of the submitted comments, they can be viewed at www.sec.gov/rules/s71100.htm.

Delivering Investor Documents Electronically

One somewhat murky area that the new release seeks to clarify is investor consent to electronic delivery of investor documents through a securities intermediary (*e.g.*, Merrill Lynch). This concept is known as "global consent", and the SEC has determined that this practice is allowable, provided that the consent is informed.

What makes consent informed? The SEC does not provide a hard and fast rule, however the essential concept is that intermediaries should take particular care to ensure that every investor understands that he or she is providing global consent to electronic delivery of all documents. Such care, according to the SEC, would likely go beyond a mere provision of an agreement that an investor is required to sign in order to obtain other services.

To best inform investors, the SEC says that broker-dealers could obtain global consent from a new customer through an account-opening agreement that contains a separate section with a separate electronic delivery authorization, or through a separate document all together. However, global consent would not be informed consent if the opening of a brokerage account were conditioned upon providing such consent. In addition, the SEC notes that investors providing global consent should be made aware of their right to revoke consent at any time and receive all documents in paper format.

As a corollary item, the SEC has determined that an issuer or market intermediary may obtain informed consent telephonically, as long as a record of that consent is retained. To ensure authenticity, the record of telephonic consent should contain as much detail as any written consent would, including whether the consent is global and what electronic media will be used.

Avoiding Improper Online Offerings

Let's say now that you are an issuer and an investor of yours has provided global consent to electronic delivery of all documents. How do you make certain that the documents you deliver to the investor electronically do not contain impermissible "free writing" - a communication that would constitute an offer to sell a security without providing a valid prospectus.

The concern here involves what is known as the "envelope theory." The SEC's envelope theory presumes that documents in close proximity (or hyperlinked) on the same Web site are considered delivered together as if they were in the same paper envelope.

The original purpose of the SEC's envelope theory, originally introduced in the SEC's 1995 Release, was to assure issuers and intermediaries using electronic media as a means to meet their delivery obligations, that they were delivering multiple documents simultaneously to investors when so required by the federal securities laws.

However, some cautious issuers (and their attorneys) expressed concern that if a prospectus were posted on an issuer's Web site then by operation of the envelope theory everything on the Web site would become part of the prospectus. The SEC has addressed this concern by stating that information on a Web site would be part of a prospectus "only if an issuer acts to make it part of the prospectus."

Dealing with Hyperlinked Information

Regardless of whether a hyperlink is considered part of an issuer's prospectus, the SEC makes issuers responsible for the accuracy of their statements that can reasonably be expected to reach investors or the securities markets. This may include third-party links if it is attributable to the issuer. Determining whether the information is attributable to the issuer or not depends on "whether the issuer has involved itself in the preparation of the information or explicitly or implicitly endorsed or approved the information."

The first part of this inquiry has become known as the "entanglement theory" and the second as the "adoption theory."

Liability under the "entanglement" theory, as the name implies, rests on the issuer's level of involvement in the preparation of the information.

Liability under the "adoption" theory may not be as clear cut, so the SEC has developed certain factors that it will use in determining whether an issuer has adopted information on a third-party Web site to which it has established a hyperlink. They include: (i) the context of the hyperlink; (ii) the risk of confusion; and (iii) the presentation of the hyperlinked information. The SEC points out that these factors are not intended to be exclusive or exhaustive, nor do they establish a "bright line" test.

Exempt Private OfferingsOnline

Another important area that the SEC touched upon is the subject of on-line exempt private offerings. The obvious concern for issuers of securities is that use of the

Continued on page 4

Concerns for Issuers SEC Speaks Again (cont'd)

Continued from page 3

Internet for exempt securities offerings may involve a general solicitation or advertising which is prohibited under the federal securities laws. For example, in an earlier release, the SEC said that an issuer's unrestricted, and therefore publicly available, Internet Web site would not be consistent with the restriction on general solicitation and advertising.

Subsequently, the SEC issued a favorable interpretive letter to a broker-dealer planning to create a password restricted Web site where qualified "accredited" or "sophisticated" investors (within the meaning of Regulation D) could take part in exempt offerings. Nonetheless, a password restricted site alone would not necessarily satisfy the SEC prohibition against general solicitation.

In addition, the SEC requires sufficient diligence on the part of the registered broker-dealer to form a reasonable belief regarding an investor's accreditation or sophistication. Merely asking investors to check a box regarding their status raises significant concerns for the SEC.

Clearly the Internet presents great potential for investors and issuers alike and the SEC recognizes this. However, it is important for issuers to move forward in this new medium vigilantly. The SEC is obviously aware of the Internet's potential and seems willing to grow and adopt as circumstances dictate. But, as the SEC has done throughout its history, change will most likely come in a slow and deliberate manner.

Lyle Mahler is an associate in the Corporate and Banking Department of Farrell Fritz and represents banks and public corporations.

Electronic Signatures (cont'd)

continued from page 1

structured format . . . perfect for insurance, banking, securities, pensions, IRA's, college savings plans and all the paper work accompanying each, along with changes in each plan or changes in beneficiaries.

The "E-Signature" law goes beyond the simple reproduction of printed documents on the Internet, by defining electronic signatures broadly ("an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."), so even telephone keypad agreements (e.g., "press 1 to agree or 3 to reject or 5 to hear menu again") are covered .

The "E-Signature" law defines electronic signatures broadly: "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

Many transactions over the Internet thrive due to the established law involving the use of the rights, obligations and liabilities of credit cards, along with a cap on loss in the event of theft or fraud. This law has enabled Amazon, CDNOW and others to thrive — once consumer confidence was established.

The new statute applies to any transaction "relating to the conduct of business, consumer or commercial affairs between two or more persons," including:

- the execution of a prototype plan
- adoption agreement by an employer
- the execution of an IRA application by an individual
- the waiver of a qualified joint and sur vivor annuity by a plan participant's spouse
- the designation of any beneficiary in connection with any retirement, pen sion, or deferred compensation plan
- a qualified State tuition program
- an insurance or annuity contract
- an agreement to transfer ownership

upon the death of a party to a transaction."

And although not all of the Uniform Commercial Code is covered, sections 1-107, 1-206 and Articles 2 and 2A are specifically brought within its scope.

Insurance regulation, even though "interstate commerce," has long been left to the States under the McCarran- Ferguson Act (with notable exceptions). Here it is accorded direct coverage with the phrase "it is the specific intent of the Congress that this title and title II apply to the business of insurance."

Banks who face costly paper check storage requirements can now comply with the new law "by retention of an electronic record of the information on the front and back of the check . . . "

Exemptions from coverage are afforded to wills, family law matters, court pleadings, utility notices, notices under leases for the primary residence of an individual and product recalls, to name a few.

For those relying on New York's Electronic Signature Act, its provisions are still applicable under the Exemption to the Preemption section, as it specifies alternate consistent procedures and does not accord any specific technology any greater legal status for electronic signatures. Thus, familiarity with both the federal and state law is necessary when using or relying upon electronic signatures.

J. Kemp Hannon is Counsel to Farrell Fritz, and the New York State Senator representing the 6th district. Senator Hannon sponsored New York State's Electronic Signature Bill, which passed into law in late 1999.

FTC Rule Protects Childrens' Online Privacy

By Eric W. Penzer
epenzer@farrellfritz.com

In March of 1998, the Federal Trade Commission ("FTC") surveyed over 200 commercial children's Web sites. Although the vast majority of the sites surveyed collected personal information from children, only a fraction of them posted privacy policies. An even smaller fraction required parental consent to the collection or disclosure of the information collected. This survey precipitated the federal government's passage of the Children's Online Privacy Protection Act of 1998 ("COPPA").

COPPA applies to commercial Web sites and online services directed to children under 13 years of age, and those that knowingly collect personal information from children. COPPA has two main requirements. First, it authorizes the FTC to issue regulations requiring the operator of any Web site or online service directed to children that collects personal information from children to provide notice of the nature and uses of the data collection. Second, it requires online services or Internet sites directed at children to obtain "verifiable parental consent" from the parent for the collection, use or disclosure of a child's personal information.

On October 21, 1999, the FTC issued its "Final Rule" to implement COPPA, which became effective six months later, on April 21, 2000. Generally, the Final Rule requires operators of commercial Web sites or online services that are entirely or even partially directed to children to:

- Provide parents notice of their information practices;
- Obtain prior verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions for the collection of contact information such as an e-mail address);
- Provide a parent, upon request, with the means to review the personal information collected from a child;
- Provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the fur ther collection of personal information from the child;
- Limit collection of personal information for a child's participation in a game, prize offer, or other activity to that reasonably necessary for the activity; and
- Establish and maintain reasonable procedures to protect the confidentiality, security and integrity of the personal information collected.

Careful scrutiny of the Final Rules is necessary to determine whether a Web site is in compliance with the rules, and whether the rules apply in the first place. By way of example, COPPA applies to any "operator of a Website or online service directed to children". However, the Final Rules provide detailed definitions of the terms "operator" and "Web site or online service directed to children." Both of these terms are of central importance in determining what entities are covered by the rules, and what Web sites fall within the ambit of the restrictions. A similarly detailed definition is provided to determine whether information collected from a child constitutes "personal information" of the type regulated by COPPA.

Moreover, care must be taken to enact and apply procedures for obtaining the "verifiable parental consent" that is required before collecting, using, or disclosing personal information. The Final Rules adopt a "sliding scale" for such consent, permitting Web sites to vary their method of obtaining consent based on the intended use of the information.

Finally, the Final Rules provide a "safe harbor" defense, allowing Web sites to obtain FTC approval of self-regulatory guidelines for compliance with COPPA. After such approval is obtained, an operator will be deemed to be in compliance with the Final Rules if that operator complies with its own guidelines. This will enable an operator to take much of the guess-work out of complying with COPPA.

COPPA is far from the last set of regulations to be implemented by the government affecting the Internet. Although care must be taken immediately to ensure compliance with COPPA and the Final Rules, certainty of compliance may require either adopting, and obtaining FTC approval of, self-regulating guidelines (to gain the protection of the safe-harbor defense), or awaiting judicial decisions clarifying the precise conduct permissible and impermissible under the Final Rules.

Eric W. Penzer is an associate in the Commercial Litigation Department and represents businesses in commercial disputes.

Partner Panelist at Turnaround Seminar for Dot-Coms

Farrell Fritz partner Ted Berkowitz will be a featured panelist at the Turnaround Management Association Long Island Chapter's October meeting, "Distressed Dot-Coms: Turnaround Situations or Liquidations?" The program will be held on Tuesday, October 10 at 5:45 p.m. at the Milleridge Cottage in Jericho.

If you are interested in attending this program, call Michael Collins of Albrecht, Viggiano, Zureck & Company at (631) 434-9500.

The Turnaround Management Association is comprised of accountants, attorneys and other turnaround professionals.

Appointment to Cyberspace Committee

James M. Wicks, Farrell Fritz partner and Editor of *TechLaw,* was recently appointed as a member of the New York State Bar Association's (NYSBA) Special Committee on Cyberspace Law. The NYSBA Executive Committee endorsed the creation of this committee to focus on legal implications faced by attorneys dealing with emerging technologies.

Partner to Speak at Suffolk Academy of Law

Farrell Fritz partner **James Wicks** will be a featured speaker at "Litigation in an Electronic World: Cyberlaw Issues & the Uses of Technology in Discovery and Trial," a Suffolk Academy of Law program to be held on Tuesday, November 14 at 6 p.m.. Ilene Cooper, Counsel at Farrell Fritz, is the program coordinator, which also includes the Honorable William D. Wall, U.S. Magistrate Judge. Practicing attorneys will receive 3 MCLE credits. For more information, call the SCBA at (631) 234-5588.

techLAW

techLAW is published quarterly by Farrell Fritz, P.C. Farrell Fritz, one of Long Island's largest law firms, serves large and small businesses, institutions, municipalities and individuals in corporate, banking, litigation, real estate, new media, land use, environmental, bankruptcy, tax, employment and trusts and estates matters.

If you have any comments or suggestions, please contact our Editor, James M. Wicks.

Editor
James M. Wicks, Esq.
(516)227-0617
jwicks@farrellfritz.com

Managing Editor
Melissa Kane, Marketing Director
(516) 227-0623
mkane@farrellfritz.com

Farrell Fritz, P.C.
EAB Plaza
Uniondale, NY 11556
(516) 227-0700
www.farrellfritz.com

Liability for the Linker

continued from page 1

case included a number of Web sites which first posted the actual DeCSS program and, when a preliminary injunction was issued against this posting, linked to other sites on which the software was posted.

In its decision, based upon §1201(a)(2) of the Copyright Act, part of the Digital Millennium Copyright Act, the Court found the defendants had offered, provided or otherwise trafficked in technology "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to" a copyrighted work. The Court rejected defendants' arguments that the distribution of DeCSS had significant non-infringing uses, or that the code constituted speech protected under the First Amendment. Regarding the linking, the Court noted that the defendants linked both to sites containing the illegal material as well as to the actual file contained on other servers, but found the linking to be "offering, providing or otherwise trafficking" in accordance with the DMCA. The Court argued that because the defendants were specifically reacting to the preliminary injunction which prohibited them from posting the code directly, and because the linked-to sites were actually encouraged to post the material and then linked-to, the fact that it did not reside on defendants' own sites was not enough to shield them from liability. The Court ordered an immediate cessation to any linking or posting of the DeCSS software.

The case is likely to be appealed, so its final impact cannot yet be determined. It is worth noting, though, that this case like a few others in the past year where liability was found due to linking, also contains an element of attempting to avoid a court's prohibition on direct distribution of material by providing or encouraging the posting of the material elsewhere and then linking to the posting sites. The Court in this case does draw some distinctions between linking to sites which happen to contain infringing materials, and doing so with the specific intention of encouraging access to the materials. Farrell Fritz will keep you informed as this case and others like it proceed.

Jonathan I. Ezor is of counsel to Farrell Fritz, and is Director of Legal Affairs for Mimeo.com, an Internet document reproduction, binding, and delivery company headquartered in New York City.

Seminar Explores Workplace Privacy

On Wednesday, October 8, Farrell Fritz partner **Kathleen Tomlinson** will be leading a seminar called "Privacy Issues in the Electronic Workplace" at C.W. Post from 8:30 until noon. Partner **James Wicks** will be among the speakers featured during the morning. Topics covered will include:

- Expectations of Privacy Among Today's Baby-Boomer to Generation X Workforce
- The E-Signatures Act
- Parameters of Employer's "Search and Seizure" Rights in Today's Workplace
- Inherent tensions in the Electronic Communications Privacy Act
- "Secret Workplace Snooping" and the proposed Notice of Electronic Monitoring Act pending before Congress
- Credit Checks and Employee Investigations: living with the Fair Credit Reporting Act
- Lie Detectors, Drug Tests, Video Surveillance, Genetic Testing, Fingerprinting - what is a reasonable personnel policy?

If you are interested in attendingthis cutting edge seminar, please contact the C.W. Post School of Continuing Education at (516)299-2236. The seminar fee is $40.

Counsel Speaks Out on Legal Issues

Farrell Fritz Counsel **Jonathan Ezor** is again on the Internet lecture circuit. Jonathan will be at the Internet World conference, in New York on October 25, speaking about "Legal Risks for Affiliate Marketers." On November 15, Ezor will be speaking to the Long Island Chapter of International Association of Business Communicators breakfast, and on November 16, he will be a featured panelist at the Bloomberg/EAB small business breakfast on e-commerce in New York. Mr. Ezor will start next year's lecture tour at the January 11 American Marketing Association Luncheon Meeting, speaking about "the 1-to-1 promise" in New York City.