Cyber Torts: Common Law and Statutory Restraints in the United States

Gregory C. Mosier and Tara I. Fitzgerald *
Oklahoma State University
Spears School of Business
Stillwater, Oklahoma 74078
Greg.Mosier@okstate.edu

Abstract
United States state courts administer common law principles that remedy injuries that arise from tortious activities. Federal statutory restrictions and overbroad federal court rulings have created immunity for many activities in the context of cyberspace. This paper reviews a number of state court decisions in the United States and surveys several basic tort principles in regard to their application to technology enhanced activities on the Internet. Tort concepts, under traditional common law concepts can, if left unrestricted, develop to serve multiple interests.

Introduction

In the United States, one of the typical domains of states and their courts, is to make determinations under their common law that provide rules related to torts and recovery for injury to persons and property. A variety of constitutional and judicial authorities support that role. Technology and the Internet have allowed new types of interaction and transactions between individuals that are not always benign and may cause injuries giving rise to tort claims in a way not previously contemplated. Of course, the strength of the common law system is its ability to evolve and develop as society and technology changes.

Clearly, concepts embodied in local, national and international legal regimes address some of the possible transgressions that may give rise to criminal penalties and, in some cases, civil liability. These statutory, regulatory and treaty based rules generally involve, at some level, deliberations that considered the impact of technology and favored policies and often are directed at such cases when passed.

In the case of the common law, the evolution of liability concepts and determination of their applicability through analogy has created a higher degree of uncertainty. To add to this uncertainty in the United States, there are federal statutory provisions that obviate the applicability of common law torts concepts. The extent to which tort law has evolved to continue its traditional redress for individuals injured by the wrongful acts of others has been severely restricted in the case of some torts, particularly when the act is one involving third party content and service providers. As Rustad and Koenig (2005) noted, despite "rosy prediction that new torts were on the horizon to protect consumers in cyberspace. We were mistaken. Tort law has yet to expand to defend the consuming public against a wide variety of wrongdoing on the World Wide Web because of the overly broad immunity conferred on ISPs."

In the United States, federal restrictions provide immunity for many activities in the context of cyberspace. Many of these activities have been traditionally governed and adjudicated according to common law tort principles. When the cases relate to property interests, the common law is adapted. When the torts alleged relate to individual interests, federal laws and the expansive interpretation of their application have limited the evolutionary path of the common law. This paper reviews a number of state court decisions in the United States and their representation of the application of basic tort principles, first to personal interests and then to property interests involving technology enhanced activities on the Internet.

1. The Communications Decency Act and Tort Claims for Injury to Person: Third Parties, Legislation and Turmoil

In *Doe v. AOL, Inc.* (2001), the State Supreme Court of Florida was called upon to provide answers to a "question of great public importance." The issue was whether or not the Communications Decency Act (CDA) had preempted certain state common law tort actions. The questions were based on a case filed by the mother of a minor child, who alleged that AOL was negligent in its oversight of its service when it failed to recognize

* A version of this paper was published in Kierkegaard, S. (2006) Business Law and Technology Vol.1 and presented at the 2006 IBLT Conference , Denmark.

or take action against a subscriber who was using the service to market and distribute child pornography. Emotional injuries were suffered by the plaintiff's son when the offender used the service to lure him to participate in his activities. The trial court and intermediate court of appeals dismissed the plaintiff's action, citing prevailing federal case law under the CDA. Section 230 of that act provides:

"(c) Protection for "Good Samaritan" blocking and screening of offensive material
(1) Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
(2) Civil liability
No provider or user of an interactive computer service shall be held liable on account of--
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) Any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).
(d) Effect on other laws
(1) No effect on criminal law
Nothing in this section shall be construed to impair the enforcement of section 223 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18, or any other Federal criminal statute.
(2) No effect on intellectual property law
Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.
(3) State law
Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."

The court rephrased the certified questions submitted to it and considered them in reverse order. It first answered the question if section 230 preempted state law negligence claims against Internet Service Providers (ISPs) as a distributors of information that violated state criminal statutes prohibiting the distribution of obscene and pornography material. Citing *Zeran v. America Online, Inc.* (1997), it then said if the premise of the law suit, based on negligence, was accepted, the question of whether or not the federal statute preempted the suit would be answered in the affirmative based on established case law from the federal courts.

The court determined that the CDA's application was indeed retroactive and applied to cases filed after the effective date of the statute, based on facts that had occurred before. The court found compelling language in the statute that stated, "no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." Such language it determined was preemptive in nature as it referred to the filing of actions and not to a post enactment activity such as preemption or "no effect" of state law. The Florida Supreme Court affirmed the lower court's decision and held that the state law's claims for negligence were preempted by the CDA.

Three of the seven judges on the court dissented in this case. Their opinion reflects discomfort with following the line of reasoning developed in federal courts, particularly *Zeran*, in interpreting the CDA. The dissent noted, "it may be somewhat attractive for the majority to follow an existing published opinion from a different jurisdiction; however, I conclude that, because the analysis upon which it is based is faulty and leads to a totally unacceptable interpretation, it should not be followed." The dissent argued that the interpretation of the CDA by state courts, following *Zeran* and its progeny to be erroneous in light of the lack of a clear pronouncement by the United States Supreme Court. It also conflicted with what it interpreted to be the legislative history of the CDA.

The *Doe* dissent can be perceived as a slight from the federal government in its attempt to regulate areas of traditional state law. It continued, with some severity, noting that, "through the majority's interpretation, the so-called "Decency Act" has, contrary to well-established legal principles, been transformed from an appropriate shield into a sword of harm and extreme danger which places technology buzz words and economic considerations above the safety and general welfare of our people."

The dissent noted many concerns with the decision of the majority, including its apparent disregard of the common law related to tort actions for defamation. Its primary focus, however, was on the legislative

history and intent of the CDA. It stated the statute was clearly directed at changing the outcome of the case of *Stratton Oakmont v. Prodigy* (1995), where an Internet Service Provider was found liable under traditional common law concepts of defamation as a publisher when it exercised general editorial control over what was posted on its web site. The purpose of the CDA, according to the dissent, was to protect such 'Good Samaritans' when they exercised blocking and screening of materials posted on their web sites.

In a caustic conclusion, the dissent stated, "Given the precise, limiting language of the statute, the stated policy underlying the CDA, and the CDA's explicit legislative history, it is inconceivable that Congress intended the CDA to shield from potential liability an ISP alleged to have taken absolutely no actions to curtail illicit activities in furtherance of conduct defined as criminal, despite actual knowledge that a source of child pornography was being advertised and delivered through contact information provided on its service by an identified customer, while profiting from its customer's continued use of the service."

In the *Zeran* case, which was relied upon by the majority in Doe, the plaintiff was injured when an unknown person posted on America Online, electronic notices of information attributed to Zeran, and advertised for sale items that glorified the 1995 bombing of the United States federal building in Oklahoma City, Oklahoma. Zeran received numerous threats as a consequence of this information and requested the information to be removed. AOL removed the notice when it was first made aware of its existence, but failed to remove the subsequent notices in a timely manner. Phone calls, abusive messages and even death threats were directed at Zeran as a result of the bogus notices. He filed suit against AOL alleging negligence as a distributor of defamatory information.

The court addressed the applicability of the CDA and referenced the preemption of state actions provision. It noted that preemption is a statutory interpretation question and in this case, Congress had not made an explicit expression of the scope of preemption it intended in the CDA. Therefore, it concluded, Congress had not intended to preempt all state law causes of action related to computer services. The court continued by noting that in this particular case the federal statute did in fact preempt the application of start law principles of torts because of the explicit language of the statute.

On a line of reasoning that has subsequently drawn a large amount of criticism, the court concluded that there is no effective difference between publisher liability and distributor liability in the law of defamation under the CDA and therefore AOL had no liability as a distributor of defamatory information under the CDA even if it was aware of the defamatory nature of the postings on it electronic bulletin boards. Since the *Zeran* case, others have addressed the issue and continued to give it deference, while acknowledging the compelling nature of interpretations to the contrary in a variety of ways

Perhaps the most prominent intentional tort that has been alleged to have arisen because of online conduct is defamation. The ease of "publishing" to the Internet makes it tantalizing for people with a grudge, malicious motives or in some cases for purposes of a mere practical joke, to utter false statements about someone that has the effect of subjecting them to the negative consequences of defamation. Under the CDA, the initial defamatory statement will impute liability to the person who makes it, as pointed out by Rustad and Koenig (2005), "in the vast majority of consumer injury cases, the injured party does not even file a claim against the anonymous wrongdoers because they are not locatable."

For example, in *Barrett v. Fonorow (*2003), the court considered a state law cause of action for defamation that was filed against a web site operator. The defendant had posted stories and articles alleged to be defamatory to the plaintiff, Barrett, who operated a web site under the domain name www.quackwatch.com. On that site, he purports to keep the public informed about a variety issues related to medical malpractice, fraudulent medical practices and targeted specifically alternative medicines. The author of the stories was critical of Barrett and the web site operator posted the stories, without edit, as provided by the author.

In considering the state law defamation claim, the court noted that section 230 of the CDA precluded claims under state law against computer service providers who use information provide by third parties. The principle issue then became whether or not Fonorow, through Intelisoft Multimedia, Inc. a corporate entity, was in fact a computer service provider. The plaintiff alleged that computer service provider means an entity that provides access to the internet. The state intermediary court quickly disposed with this argument noting that "we find (this claim) refuted by the plain text of the Act. An "interactive computer service" is defined as any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet. The definition includes, but is not limited to, Internet providers."

The plaintiff then alleged that the CDA did not preclude liability in cases where the defendant knew or had reason to know of the about the defamatory nature of the statements provided by third parties. The court then reviewed the common law elements of defamation in light of the language used by Congress in the CDA.

To state a case for defamation, the plaintiff must allege: "(1) the defendant made a false statement about the plaintiff; (2) there was an unprivileged publication of the statement; and (3) the plaintiff was damaged from the publication." The CDA in Section 230(c)(1) provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The court concluded that the language of the statute clearly was targeted at the second requirement of defamation and that the publication element was preempted. It said, "Barrett admits, and we have confirmed, that every state and federal court to confront the issue in a published decision has held that Congress intended section 230 to prevent the element of "publication" from being satisfied in a state tort cause of action where a provider or user of an interactive computer service disseminates information provided by another information content provider."

The plaintiff, in his final contention attacking the application of the federal legislation to preclude his state law claim, stated that the state court, under established state precedent, should show know no deference to the federal court decisions that provide such blanket immunity to computer service providers. The court noted a line of precedent that gave plausibility to the plaintiff's claim. It noted that in the case of *Hinterlong v. Baldwin.* (1999), in interpreting a federal statute, this court remarked that "state courts are not bound to follow decisions of the federal district courts or circuit courts of appeal." It concluded however, that more relevant to the situation at hand are the several recent Supreme Court cases explaining the degree of deference owed by Illinois courts to federal cases interpreting federal statutes. In *Wilson v. Norfolk & Western Ry. Co.* (1999), the court said: "The reason that federal decisions are considered controlling on Illinois state courts interpreting a federal statute is so that the statute will be given uniform application."

The court then dealt with the issue of whether or not the defendant's claim for sanctions against the plaintiff should be granted. The court rejected imposing sanctions on the plaintiff, noting, "The interpretation introduced by the Fourth Circuit in *Zeran*, and now prevailing in the federal courts, has been vigorously criticized by many legal commentators as a license for defamation on the Internet that was not intended by Congress. Based on the statute and its historical context (examined intensively by these commentators), we, too, find it plausible that Congress did not intend blanket immunity for those who disseminate the false and defamatory statements of third parties over the Internet."

In a pending California Supreme Court case, Barrett is once again involved in a law suit, claiming he and a colleague were defamed by alternative health care advocates. In *Barrett v. Rosnethal* (2003), Barrett and an associate, Terry Polevoy, were allegedly defamed by an alternative medicine advocates utilizing Usenet newsgroups. In a series of postings, an adversary of the plaintiffs reposted communications she had received from another person on the Usenet forums. Allegation in the posting included those of criminal misconduct by one of the plaintiffs. When notified of the false nature of her postings, the defendant, Rosenthal, refused to remove them and distributed them more widely along with the plaintiffs' demands. Litigation ensued.

At trial, among other rulings, the judge found that the statements, reposted by Rosnethal, were protected by section 230 of the CDA regardless of the fact the plaintiffs may have been able to prove the relevant elements of defamation under state law. The plaintiff's actions were all summarily dismissed. The appellate court, in reviewing the trial courts decision, related to the CDA, stated, "we find that the immunity available under section 230 does not bar the imposition of liability in this case, that malice and reckless disregard for the truth can be inferred from the circumstances, which include the failure to conduct a reasonable investigation regarding the truth of the accusation of criminal conduct and reliance on obviously biased sources, and that Polevey was not required to plead special damages, as the republished statement was libelous per se."

In narrowing its discussion of the ruling, the appellate court noted that the central issue in the case was to what extent the CDA preempts the common law related to defamation. In its analysis, it focused on the common law distinction between publishers and distributors. The court noted "distributors (sometimes known as secondary publishers), whose ability to control defamatory speech lies somewhere between that of primary publishers and conduits, are subject to an intermediate standard of responsibility and may only be held liable as publishers if they know or have reason to know of the defamatory nature of matter they disseminate." The court continued by noting the reliance on Z*eran* as a leading case for the proposition of absolute immunity for computer service providers under section 230. It then, after reviewing the facts in that case, noted the flaws most commonly found with that court's reasoning.

The *Zeran* court had asserted that, "Congress recognized the threat that tort based lawsuits pose to freedom of speech in the news and burgeoning Internet medium the imposition of tort liability on service providers for the communications of others represented, for Congress simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature on internet communications and accordingly, to keep government interference in the medium to a minimum." The *Zeran*

court continued, ″none of this means of course that the original culpable party who posts defamatory messages would escape accountability."

The Barrett appellate court was not persuaded by the reasoning in *Zeran*. From challenging the overbroad purpose attributed to the statute by the court, noting a basic misunderstanding of the common law of defamation and to finally to ignoring the common law principle that statutes in the derogation of the common law are to be strictly construed, the court rejected the reasoning from that case. Citing the Supreme Court in the case of *United States v. Texas (*1993), it said "in order to abrogate a common-law principle, the statute must speak directly to the question addressed by the common law. Continuing with a critique of the *Zeran* case and a thorough review of the scholarly discussion surrounding the decision, the court concluded that section 320 did not bar the defamation claim against a common law distributor of defamatory material.

After the appellate court's opinion, the case was appealed to the California Supreme Court and the decision was reversed. Citing the prevailing case law based on *Zeran*, the California Supreme Court noted the reasons often given for absolute immunity. They include the following:

- a potential chill on internet freedom of speech;
- a contrary ruling might deter computer service providers from screening;
- "Online Hecklers" might be empowered; and
- an invitation to open forum shopping in jurisdictions that recognize a cause of action.

2. Torts against Property: No Statutory Confusion

In some cases, common law tort principles have evolved with due consideration given to modern technologies and circumstances. These cases represent the ability of such concepts to adapt. The following state court decisions are illustrative of the application of traditional common law tort principles in cyberspace where personal property interests are still deemed protected by state laws unlike the decisions regarding personal interests discussed above. By their nature, the claims relate to property interests and in most cases represent the interests of business. The following cases depict the expected evolution of property concepts with regard to new technology and personal property definitions. It is well settled that the underlying elements and definitions required for such tort actions come from state common law. Federal legislation has not interfered with state court authority on these matters. The cases address the application of traditionally accepted personal property tort law concepts under Conversion, Misappropriation of Trade Secrets and Trespass Chattels to cyberspace related types of property. They represent the types of cases identified by Rustad and Koenig (2005): "Repeat player corporations tower above other plaintiff categories in litigation over personal property torts in cyberspace. Nearly a quarter of the cases in the sample were trespass to chattels or conversion actions filed by ISPs or other repeat players against spam e-mailers or fraudulent cyberpirates."

2.1 Conversion

The New York Supreme Court in *Shmueli v. Corcoran Group* (2006) was called to decide whether a computerized list (an electronic document that exists inside a computer as opposed to a tangible document that exists on a piece of paper) can be subject to the tort of conversion. The plaintiff in the case alleged that upon termination of their business relationship, the defendant wrongfully denied plaintiff access, and continues to deprive plaintiff access, to various real estate deal and client lists she maintained on the computer furnished to her by defendants. The defendant claimed the common law tort of conversion cannot be applied to intangible property. The decision and rationale in this case exemplify the application and expansion of cornerstone legal principles to new situations found in our highly technical modern world.

The court found that the tort of conversion, that is the wrongful exclusion and retention of a rightful owner's physical property, does apply to an electronic record created by a plaintiff to the same extent it would to a paper record created by a plaintiff. The court explained that a computerized list can "undeniably transform" to a physical document simply by utilizing the printing function of the computer. It reasoned that the common law tort of conversion should not become "extinct" in application to documents maintained on a computer, but should "evolve" in sync with the definitions of documents over time. The recording of data and the creation of documents is not limited to paper. The tort of conversion must respect progress in technology and continue to provide redress when one wrongfully interferes with the ownership of electronic documents.

Although the court in this case admitted that the traditional application of this common law cause of action has "always centered exclusively on the physical theft of specific, identifiable, corporeal, tangible, personal property", the court went on to explain that when the nature of tangible personal property expanded to include tangible documents that represent intangible rights, such as bank notes, promissory notes, stock certificates, and insurance policies, courts began to interpret the tort of conversion to include these paper documents within its scope. Citing *Hartford Accident & Indem. Co. v. Walston & Co., Inc.* (1967), the court said that the New York Court of Appeals followed the trend when it applied the tort of conversion to the theft of stock. The court in this case found no reason why it should not apply the same logic to the present type of documents. Electronic documents belong to someone and are subject to theft. Therefore, it fell within the scope of the tort of conversion.

The court also referred to two federal decisions and agreed with their reasoning. In *Kremen v. Cohen* (2003), the Ninth Circuit permitted the plaintiff's conversion claim regarding its Internet domain name. In *Astroworks, Inc. v. Astroexhibit, Inc.* (2003), the District Court for the Southern District of New York allowed the plaintiff to sue the defendant for converting plaintiff's ideas for an Internet, web-based business to defendant's own gain. The intangible nature of the property involved in these cases did not preclude a cause of action for conversion. The court in this case agreed that the historic distinction between tangible and intangible property must be less rigidly applied in order to "keep up with science."

The finding in this case- "that electronically written 'documents' should not be treated with less dignity of ownership for conversion purposes than ink written 'documents" was upheld on appeal by the New York Supreme Court Appellate Division.

2.2 Misappropriation of Trade Secrets

In *Briefing.com v. Jones*, the Supreme Court of Wyoming agreed to answer the following two questions submitted by the United States District Court for the District of Wyoming: "1. Would the Wyoming Supreme Court adopt a common-law cause of action for misappropriation of trade secrets and/or confidential information when the former employees of a company are alleged to have misappropriated their former employer's trade secrets and/or confidential information to start a competing business? 2. If the answer to question number 1 is yes, what are the elements of the cause of action?" The questions resulted from a diversity case filed by a California corporation, an Internet based company that provides stock and fixed income markets analysis for individual and professional investors on its website, against two of its former employees who are Wyoming residents.

The plaintiff alleged that the defendant's utilized trade secrets and/or confidential information gained in their positions with the plaintiff to form and operate a competing business. Specifically the plaintiff claimed that the defendants had access to confidential information and data with respect to the internet based market analysis trade, knowledge of the plaintiff's development and proprietary studies regarding designs and themes and access to market contact information.

The state of Wyoming had not previously considered a case regarding the protection of trade secrets and consequently had not addressed the issue with respect to intangible electronic information and an Internet based company.

The court answered the first question in the affirmative: that common law in the state of Wyoming includes a cause of action for misappropriation of trade secrets and/or confidential information with regard to information gained during employment and used to start a competing Internet business. The court responded to the second question and ruled that the elements required to support such a cause of action are those found in the restatement (Third) of Unfair Competition. The court reasoned that misuse of trade secrets is a recognized cause of action under common law and that the Wyoming legislature had adopted the common law as applicable in Wyoming more than 100 years ago. In determining the elements of the tort, the court referred to the Restatement (Third) of Unfair Competition and stated that it served to "accommodate the law to developments in the commercial world."

2.3 Trespass to Chattels

To establish a common law action for trespass to chattels, a plaintiff must prove that the defendant intentionally and without consent, physically interfered with the use and enjoyment of personal property in the plaintiff's possession, and that the plaintiff was thereby harmed. The interference with the chattel must have resulted in harm to the owner's interest in the physical condition, quality or value of the chattel, or when the

owner is deprived actual use of the chattel for a substantial period of time. In *School of Visual Arts v. Kuprewicz* (2003), the Supreme Court of New York determined whether the common law trespass to chattels applies to a computer system. The plaintiff alleged that the defendant, a former employee, caused "large volumes" of unsolicited job applications and pornographic emails to be sent to School of Visual Arts' (SVA) computer system, without their consent. The plaintiff further alleged that these unsolicited emails "depleted hard disk space, drained processing power, and adversely affected other system resources on SVA's computer system." The court found that the plaintiff had stated a valid cause of action for trespass to chattels.

The court cited several cases where such a cause of action had been applied to computer systems. In CompuServe *Inc. v. Cyber Promotions, Inc.* (1997), the sending of unsolicited commercial bulk emails supported a claim for trespass to chattels where processing power and disk space were shown to be adversely affected, and in *Hotmail Corp. v. Van$ Money Pie Inc. (*1998) the plaintiff was determined likely to prevail on a trespass to chattels claim upon having shown that plaintiff's computer storage space was filled up by the defendant's unsolicited emails.

In order to prevail with respect to an action for trespass to a computer system, a plaintiff must show that the chattel suffered physical damage. Damage to objects traditionally found in trespass to chattels claims is usually visible and easy to establish. However, the court stated that if physical damage, albeit invisible damage, occurs to the computer system, the plaintiff has a cause of action.

Torts that protect property interests, such as conversion, misappropriation of trade secrets and trespass to chattels, can also apply to our highly technical world. Electronic documents, intangible information and invisible systems deserve the same protections as tangible personal property. Courts must modernize their views of the definition of "property" to include these intangible and invisible aspects created by technology

3. Conclusion

Traditionally, when individuals have been injured by the wrongful act of another person, they have recourse through the common law concepts of tort law to seek redress. While technology has allowed access to a variety of ways to facilitate beneficial activities, it has also allowed types of injurious behavior that are the inevitable result of personal interaction and human conduct. In the United States, the state courts have followed age old tradition in developing and evolving the legal concepts in such as to incorporate new situations and circumstances into established legal principles. In the case of torts committed in cyberspace, the development of the common law of torts related has been abruptly halted when it involves a third party, computer service provider. In these cases, the types of injuries typically alleged are those against the person. In the case of torts against property, claims are typically directed against a primary or direct tortfeasor and the liability has remained intact.

When cases involve the Communications Decency Act (CDA) and its preemption of state law claims, clearly the preemption applies to such claims against computer service providers who utilize content provided by another. Limited actions would obviously be available against the primary provider, who in many cases may have insufficient resources to satisfy claims. The United States Supreme Court has not ruled on the issue. While the current sentiment of courts is to follow the line of reasoning that would give absolute immunity to all computer service providers who utilize materials or information provided by others regardless of knowledge, pending litigation can provide a new interpretation that may be persuasive to courts that have not considered the question.

When state courts have followed the traditional methods of analogy, *stare decisis* and evolution of principles, such as those involving torts against property in cyber space, the common law has proven robust, leading to decisions that consider precedent while maintaining relevance and innovation. Legislative attempts at "fixing the common law" and its outcomes typically are driven by policy reasons that have diverse rationales. In the case of the CDA and the court in *Zeran,* those considerations include removing "disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material" and concern about a potential flood of tort claims that overwhelm computer service providers.

The common law, even with its multiple state systems in the United States, has a tradition of considering such issues and folding them into a vibrant system protecting many interests. Legislations, such as the CDA, should be interpreted in light of basic common law principle- "statutes in the derogation of the common law should be strictly construed." Then in the case of cyber space, state courts will reclaim the common law of torts.

References

1. Astroworks, Inc. v. Astroexhibit, Inc., 257 F.Supp.2d 609 (SDNY 2003).
2. Barrett v. Fonorow, 799 N.E.2d 916 (Ill. App. 2003).
3. Barrett v. Rosnethal, 112 Cal. App. 4th 749 (2003).
4. Briefing.com v. Jones, 2006 WY 16, 126 P.3d 928 (2006).
5. Communications Decency Act, 47 U.S.C. § 230(c) (1) (2000).
6. CompuServe Inc. v. Cyber Promotions, Inc., 962 F.Supp 1015 (SD Ohio 1997).
7. Doe v. AOL, Inc., 783 So. 2d 1010 (Fl 2001).
8. Hartford Accident & Indem. Co. v. Walston & Co., Inc., 234 N.E.2d 230 (1967) adhered to on rearg 238 N.E.2d 754 (1968).
9. Hinterlong v. Baldw, (Ill. App. 1999).
10. Hotmail Corp. v. Van$ Money Pie Inc., WL 388389 (1998).
11. Kremen v. Cohen, 337 F.3d 1024 (9th Cir 2003).
12. Restatement (Second) of Torts.
13. Restatement (Third) of Unfair Competition.
14. Rustad, M., & Koenig, T. (2005). Rebooting Cybertort Law. *Washington Law Review*, 80.
15. School of Visual Arts v. Kuprewicz, 771 N.Y.S.2d 804 (2003).
16. Shmueli v. Corcoran Group, 802 N.Y. S.2d 871 (2006).
17. Stratton Oakmont Inc. v. Prodigy, (N.Y.Sup.Ct. 1995).
18. United States v. Texas, 507 U.S. 529 (1993).
19. Wilson v. Norfolk & Western Ry. Co., 718 N.E.2d 172 (Ill.1999).
20. Zeran v. America Online, Inc., 958 F. Supp. 1124, (E.D. Va. 1997).