

1 of 1 DOCUMENT

Copyright (c) 2000 The University of Toledo
Toledo Law Review

Spring, 2000

31 U. Tol. L. Rev. 347

LENGTH: 15898 words

ARTICLE: POLICIES UNDERLYING CONGRESSIONAL APPROVAL OF CRIMINAL AND CIVIL IMMUNITY FOR INTERACTIVE COMPUTER SERVICE PROVIDERS UNDER PROVISIONS OF THE COMMUNICATIONS DECENTY ACT OF 1996 - SHOULD E-BUYERS BEWARE?

NAME: Mary Kay Finn,* Karen Lahey,** and David Redle***

BIO: * Mary Kay Finn is a lawyer and assistant professor of business law at The University of Akron, College of Business Administration, Akron, Ohio. The author gratefully acknowledges the contributions of Jason Butterworth, graduate assistant at the College and a student of The University of Akron Colleges of Law and Business Administration.

** Dr. Karen Lahey is a Professor of Finance at The University of Akron, College of Business Administration, Akron, Ohio.

*** David Redle is a lawyer and Department Chair at the University of Akron, College of Business Administration, Department of Finance.

SUMMARY:

... SIGNIFICANT discussion has recently focused on the demand for meaningful regulation of what is known as "e-commerce," or trade that is conducted via the Internet through forums such as eBay.com, AuctionUniverse. ... Of the total number of complaints concerning Internet fraud filed with the National Consumers League in 1998, five thousand two hundred thirty-six, or slightly more than two-thirds, were related to online auction fraud. ... Based on the sheer volume of information ISPs receive and maintain daily, much has been made of the difficulty, if not impossibility, of effectively monitoring the content of messages sent over the Internet and through electronic bulletin boards. ... Internet business traders, particularly online auction houses, seek to use contractual limitations to achieve the same goal. ... On February 1, 1999, the District Court for the Eastern District of Pennsylvania permanently enjoined this revised attempt to regulate Internet content under the auspices of the First Amendment. ... In the final analysis, Senate Bill 652 created new defenses to assure that the mere provision of access to an interactive computer service or good faith monitoring or filtering of content did not create liability. ... First, holding auctioneers responsible for fraudulent content might have a chilling effect on constitutionally protected commercial speech, particularly where it is clear that Congress does not wish to unnecessarily tether Internet development. ...

TEXT:

[*347]

SIGNIFICANT discussion has recently focused on the demand for meaningful regulation of what is known as "e-commerce," or trade that is conducted via the Internet through forums such as eBay.com, AuctionUniverse.com, uAuction.com and, most recently, Amazon.com. Of particular concern to consumers is the issue of fraud in this rapidly

growing forum of exchange. Overall, \$ 2.1 billion of the \$ 13 billion in Internet commerce conducted last year was attributable to online auctions, with analysts expecting sales to triple by 2000.ⁿ¹ Recognizing that the Internet provides fertile ground for fraud upon the direct participant, Internet service providers (ISPs) such as America Online are moving, legislatively and contractually, to protect themselves from various forms of liability, including fraud. It is apparent that traditional lines of dispute between buyer and seller similarly are being drawn, adding a twist with third party conduits like online auctions. While it seems appropriate to allow reasonable limitation of liability for these forums in traditional contract terms, attempted limitations stretch into less appropriate areas. As history has shown, commercial abuse often results in regulation, or attempted regulation, of the activity. Using the legislative history of the Communications Decency Act of 1996 as a policy platform, this article explores the probability that parallel policies will persuade Congress to insulate ISPs and other mere conduits of information, like online auctions, from liability for fraudulent and criminal consumer fraud, underscoring that the buyer should indeed beware.

I. Introduction

Significant discussion has recently focused on the call for oversight or regulation in the e-commerce area. In short, e-commerce is the term applied to conducting business or trade through the Internet. For purposes of this article, trade conducted by online auction houses such as eBay.com, Auction Universe, uAuction, Yahoo!, and, most recently, Amazon.com will be examined. Despite notable efforts by [*348] forums like eBay.comⁿ² (eBay) to validate users, facilitate feedback concerning dealers and buyers, and to provide nominal insurance for online buyers, online auction forums have been nonetheless the target of consumer concerns about overpriced, inauthentic and undelivered merchandise.ⁿ³ Of the total number of complaints concerning Internet fraud filed with the National Consumers League in 1998, five thousand two hundred thirty-six, or slightly more than two-thirds, were related to online auction fraud.ⁿ⁴

Despite online auctioneers' attempts to skirt liability under traditional tort principles through extensive user agreements, eBay was nonetheless targeted by the New York Department of Consumer Affairs for allegations that it fraudulently listed and sold inauthentic sports memorabilia.ⁿ⁵ In response to news of the probe, eBay vowed to cooperate, noting that it had recently stiffened anti-fraud measures by,ⁿ⁶ among other things, providing insurance to users of its site.ⁿ⁷ In particular, eBay initiated its SafeHarbor<tm>, a service designed to "promote safe online trading, as well as protect the community from fraud."ⁿ⁸ The primary features of eBay's SafeHarbor<tm> are free insurance (up to a total amount of \$ 175), user registration validation, a comprehensive and generally accessible "Feedback Forum" in which buyers and sellers can rate their transaction-related experiences, and an escrow service.ⁿ⁹ In addition, although denying any liability for fraud,ⁿ¹⁰ the eBay site includes a hyperlink to a "Fraud Prevention" page that provides information for contacting law enforcement agencies and tracking consumer complaints.

In an apparent effort to stave off imminent federal inquiry into a multitude of privacy and security issues involving Internet commerce, seventeen of the largest Internet companies (including America Online, Inc., Time Warner, Inc., IBM, Fujitsu Ltd., and Toshiba Corp.) have formed an e-commerce initiative known as the Global Business Dialogue on E-Commerce.ⁿ¹¹ Among other things, this powerful consortium will explore issues of consumer confidence on the Internet. This industry effort has prompted claims that the proverbial "fox is again guarding the [*349] hen house," and has raised concerns among consumer advocates that self-regulatory efforts will fall far short of what is needed to ensure consumer protection.ⁿ¹²

Based on the sheer volume of information ISPs receive and maintain daily, much has been made of the difficulty, if not impossibility, of effectively monitoring the content of messages sent over the Internet and through electronic bulletin boards. In an effort to protect ISPs from liability for certain "offensive" transmissions, Congress, in the Communications Decency Act of 1996ⁿ¹³ and in succeeding sections known as Online Family Empowerment,ⁿ¹⁴ immunized ISPs from liability for acting as the medium through which third parties transmit offensive or obscene material, and omitted them from the definition of a "publisher" within the context of defamation law.

Internet business traders, particularly online auction houses, seek to use contractual limitations to achieve the same goal. It is logical to suspect that online traders may ultimately argue that judicial or legislative immunity from consumer

fraud claims is necessary to foster growth and development of online trading and to guard against the chilling of commercial speech. Looking at the legislative record concerning the enactment of the Telecommunications Act of 1996, ⁿ¹⁵ we may indeed conclude that Congress may be persuaded by the fact that commerce has been buoyed by Internet auctions from both the buyer's and seller's perspectives, amid claims by some sellers that they have entirely omitted advertising and direct mail marketing expenses in favor of the global exposure provided by forums like eBay. ⁿ¹⁶ More precisely, in portions of the Telecommunications Act of 1996, referred to as the Communications Decency Act (CDA), ⁿ¹⁷ Congress was similarly concerned that imposing liability on providers and users of Internet services would quell free speech, and stifle the growth of a medium of interactive exchange whose benefits to consumers far outweigh any concerns about its shortcomings. In the end, Congress decided to immunize ISPs and users from liability for indecent communications if they merely transmitted information authored by others. In addition, Congress placed defenses to criminal prosecution and civil liability in the CDA for those ISPs who take effective, good faith measures to scrutinize communications for offensive or indecent content. ⁿ¹⁸

Based on the legislative history surrounding the original enactment of 47 U.S.C. sections 223 and 230, it is fair to anticipate that e-commerce consumers should be concerned that Congress will be similarly persuaded that immunizing commercial online auctioneers from tort liability for fraud that occurs through use of their "forums" merits serious consideration. Furthermore, if Congress does choose to immunize or provide broad good faith defenses to online auction houses, consumers [*350] should also recognize the severe limitations of common law or available statutory remedies. What will e-commerce "give" in exchange for immunity and the benefits of conducting massive amounts of commerce on the Internet? It is quite possible that Congress will approve measures like those voluntarily instituted by eBay (insurance, feedback and escrow) as an effective, good faith "hedge" against consumer losses. Even with these safeguards, however, e-consumers may be relegated altogether to the oftentimes meaningless remedy of pursuing the unidentifiable, unascertainable fraud perpetrator who existed only for a brief transaction, thereafter disappearing into the quagmire of cyberspace. ⁿ¹⁹

Using the eBay User Agreement and procedures as an example, this article explores one online business trader's attempt to insulate itself from liability. Congressional policies that resulted in the immunization of online ISPs from limited tort liability in sections 223 and 230 of Title V of the Communications Decency Act of 1996 ⁿ²⁰ are also addressed in order to determine their applicability to the online auction situation. In addition, judicial decisions applying the statute are analyzed, and policy-shaping practical issues are addressed.

Overall, the research reveals that Congress, as well as the courts, consistently conclude that due to the vast amount of information processed each day by ISPs, imposing liability on them for content provided by third parties is neither technologically nor politically feasible. ⁿ²¹

II. The eBay User Agreement

When a user accesses an online auction site like eBay, he/she is likely to encounter a comprehensive User Agreement. eBay's User Agreement illustrates the types of liability limitations users of the service are likely to encounter where online auctions attempt to protect themselves. Section 3 of eBay's Agreement provides:

3. eBay is Only a Venue.

3.1 Overview. Our site acts as the venue for sellers to list items (or, as appropriate, solicit offers to buy) and buyers to bid on items. We are not involved in the actual transaction between buyers and sellers. As a result, we have no control over the [*351] quality, safety or legality of the items advertised, the truth or accuracy of the listings, the ability of sellers to sell items or the ability of buyers to buy items. We cannot ensure that a buyer or seller will actually complete a transaction.

3.2 Safe Trading. Because user authentication on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established a user-initiated feedback system to help you evaluate with whom you are dealing. We also encourage you to communicate directly with potential trading partners. You may also wish to consider using a third party escrow service or services that provide additional user verification...ⁿ²²

In an apparent reference to eBay's estimated 1.7 million items available at any one time, section 3 continues:

3.3 Release. Because we are not involved in the actual transaction between buyers and sellers, in the event that you have a dispute with one or more users, you release eBay (and our officers, directors, agents, subsidiaries and employees) from claims, demands and damages (actual and consequential) of every kind and nature, known and unknown, suspected and unsuspected, disclosed and undisclosed, arising out of or in any way connected with such disputes. If you are a California resident, you waive California Civil Code 1542, which says: "A general release does not extend to claims which the creditor does not know or suspect to exist in his favor at the time of executing the release, which if known by him must have materially affected his settlement with the debtor."ⁿ²³

Thus, in the most comprehensive of exculpatory language, eBay insists on a contractual limitation of liability for virtually all claims and damages arising on the part of buyers or sellers. The basis for this unreasonable limitation is the fact that eBay does not "and cannot be" involved in user-to-user dealings.

The caveat continues at Item No. 6 of the User Agreement wherein eBay provides:

6. Your Information. "Your information" is defined as any information you provide to us or other users in the registration, bidding or listing process, in any public message area (including the Cafe or the feedback area) or through any email feature. You are solely responsible for Your Information, and we act as a passive conduit for your online distribution and publication of Your Information. With respect to Your Information:

6.1 Your Information (or any items listed therein): (a) shall not be false, inaccurate or misleading; (b) shall not be fraudulent or involve the sale of counterfeit or stolen items; (c) shall not infringe any third party's copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy; (d) shall not violate any law, statute, ordinance or regulation (including without limitation those governing export control, consumer protection, unfair competition, antidiscrimination or false advertising); (e) shall not be defamatory, trade libelous, unlawfully threatening or unlawfully harassing; [*352] (f) shall not be obscene or contain child pornography or, if otherwise adult in nature or harmful to minors, shall be posted only in the Adults Only section and shall be distributed only to people legally permitted to receive such content; (g) shall not contain any viruses ... Furthermore, you may not post any item on our site (or consummate any transaction that was initiated using our service) that, by paying to us the listing fee or the final value fee, could cause us to violate any applicable law, statute, ordinance or regulation, or that violates our current Prohibited, Questionable and Infringing Items (at <http://pages.ebay.com/help/community/png-items.html>) list.ⁿ²⁴

In these provisions, eBay retains editorial control over the content of listings and feedback to the extent that failure to excise or modify certain material may create liability for eBay. This section thus appears to acknowledge the potential for eBay's liability based on advertisement content. In addition, section 6.1 represents a general attempt by eBay to police the content of seller material, despite claims that this is an impossible task. Thus, eBay presents itself as a responsible participant, retaining the right to supervise content only when it chooses, without any liability for fraud, whether it undertakes to police or not.

Finally, Item No. 12 entitled, "Liability Limit," provides:

IN NO EVENT SHALL WE OR OUR SUPPLIERS BE LIABLE FOR LOST PROFITS OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH OUR SITE, OUR SERVICES OR THIS AGREEMENT (HOWEVER ARISING, INCLUDING NEGLIGENCE).

OUR LIABILITY, AND THE LIABILITY OF OUR SUPPLIERS, TO YOU OR ANY THIRD PARTIES IN ANY CIRCUMSTANCE IS LIMITED TO THE GREATER OF (A)THE AMOUNT OF FEES YOU PAY TO US IN THE 12 MONTHS PRIOR TO THE ACTION GIVING RISE TO LIABILITY, AND (B)\$ 100... n25

It is ironic that in the face of these dauntingly broad disclaimers, which appear to contractually eliminate recourse against eBay and similarly situated online auctions, the industry nevertheless flourishes. Overall, \$ 2.1 billion of the \$ 13 billion in Internet commerce conducted last year was attributable to online auctions, with analysts expecting sales to triple by 2000. n26 According to the Media Metrix, eBay was the second most visited website in December 1999, trailing only Amazon.com in the number of site visitors. n27 Consequently, it comes as little surprise that eBay posted revenues of \$ 19.5 million for the last quarter of 1998, an increase of 642% over the previous year. n28

From the consumer's perspective, it seems fair to question the appropriateness of online auctions sidestepping traditional liability under the guise that they are merely forums, though extremely profitable, for the exchange of goods. A consumers call [*353] for pervasive federal enactment designed to assert liability and preempt the contractual limitations imposed on users of such services appears inevitable. It is possible that the same public policy that underscored the need for immunity for the providers and users of interactive computer ISPs would persuade Congress to legislatively insulate online auctioneers from liability for torts like consumer fraud. An examination of the legislative history of the immunity and good faith provisions of the much-debated Communications Decency Act is helpful to this analysis.

III. Overview of the Enactment of the Immunity Provisions of the Communications Decency Act of 1996

When Senate Bill 652, eventually enacted as the comprehensive Telecommunications Act of 1996, n29 was introduced in the U.S. Senate on March 30, 1995, it generally sought to "provide for a pro-competitive, de-regulatory national policy framework designed to accelerate rapidly private sector deployment of advanced telecommunications and information technologies and services to all Americans by opening all telecommunications markets to competition, and for other purposes...." n30

The vast majority of the bill had little to do with Internet regulation. In fact, the bulk of the legislation was designed to address competition in more traditional forms of telecommunications such as the local telephone, multichannel video, and over-the-air broadcasting markets. Of the seven titles that were finally enacted, n31 six were the subject of extensive hearings and committee debate. n32 However, major portions of the last title, Title V at issue here and known as the Communications Decency Act of 1996 (CDA), n33 were added after the committee hearings were concluded. These provisions consequently were subjected to limited executive committee review or were offered directly on the floor without the benefit of extensive review and testimony from both sides of the issue. It was only after the Senate adopted the provisions that ultimately comprised the CDA that it conducted a one-day Judiciary Committee hearing in which Senator Leahy wisely observed:

It really struck me in your opening statement when you mentioned, Mr. Chairman, that it is the first ever hearing, and you are absolutely right. And yet we had a major debate on the floor, passed legislation overwhelmingly on a subject involving the Internet, legislation that could dramatically change - some say would even wreak [*354] havoc - on the Internet. The Senate went in willy-nilly, passed legislation, and never once had a hearing, never once had a discussion other than an hour or so on the floor. n34

It is fair to surmise that the apparent lack of thorough debate on the language of Title V likely contributed to its constitutional travails, discussed at length *infra*.

Aside from its procedural irregularities, a major goal of Title V was to curb the ability of children to freely access obscene or pornographic online material. The enactment thus criminalized the practice of making obscene and "patently offensive" materials indiscriminately accessible through various modes of communication, including the Internet. Not surprisingly, the floor debate on this piece of the proposed act was imbued with concerns about the constitutionality of any measure that would impede free speech.ⁿ³⁵ Many legislators expressed concern that Congress would adopt a broadly-tailored legislative prohibition to address the narrow goal of protecting the nation's children from not just obscene, but offensive and pornographic material. Congress was still "gun shy" over recent failed attempts to regulate pornography over the nation's telephone systems.ⁿ³⁶ In particular, many members feared that any type of censorship or prior restraint, no matter how justifiable, would embroil the legislation in years of litigation. For example, the ten-year battle over the federal Dial-a-Porn lawⁿ³⁷ was just recently concluded. In that litigation, Congress wearily defended its initial attempt to prohibit access by minors to pornographic information available over the telephone.ⁿ³⁸ Congress, however, was unsuccessful in that endeavor, forcing it to tackle comprehensive revisions to the law. Senator Biden artfully articulated the reticence of certain members to engage again in a protracted defense of yet another indefensible restriction on free speech:

Or put another way by Justice Frankfurter, you can't "burn the house to roast the pig" - which is exactly what I believe the Exon-Coats provision would do. So I believe there will be a heated and protracted constitutional challenge to this provision. In fact, with history as our guide, such a challenge is virtually guaranteed: when Congress banned Dial-a-Porn services to minors, it took 10 years - and many different attempts by the FCC to write narrowly tailored regulations, all of which were challenged and fully litigated, for the statute to be upheld as constitutional.

Ten years. Multiple rulemaking proceedings. Four different trips up to the court of appeals. I, for one, just can't wait that long.ⁿ³⁹

[*355] This sense of foreboding proved valid. Barely a year after its enactment, major provisions of the Communications Decency Act were ruled unconstitutional.ⁿ⁴⁰ In *Reno v. ACLU*, the U.S. Supreme Court noted that the provisions which prohibited the knowing transmission to minors of "indecent" or certain "patently offensive" communications as those terms were employed in the federal statute, under penalty of criminal fines or imprisonment, abridged the right to free speech protected by the First Amendment.ⁿ⁴¹ As a result, Congress passed significant revisions to the CDA in 1998.ⁿ⁴² As discussed *infra*, this additional attempt by Congress to address the issue of offensive or indecent Internet communications accessible to minors has already been enjoined due to constitutional defects perceived by a Pennsylvania district court.ⁿ⁴³

In sections where underlying policy was generally unaffected by the Supreme Court's decision in *Reno* and subsequent amendments, however, section 223 of the Communications Decency Act of 1996 provided defenses for the mere conduits of otherwise unlawful communications:

(e) In addition to any other defenses available by law:

(1) No person shall be held to have violated subsection (a) or (d) [which sections outlaw providing access by minors to offensive communications] solely for providing access or connection to or from a facility, system or network not under that person's control ... or related capabilities that does [sic] not include the creation of the content of the communication.ⁿ⁴⁴

Succeeding provisions stated:

(5) It is a defense to a prosecution [hereunder] ... that a person -

(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a [prohibited] communication ...ⁿ⁴⁵

(6) The [Federal Communications] Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d).ⁿ⁴⁶

+ Section 230 of the Communications Decency Act, the Online Family Empowerment law, was also amended to provide civil immunity for online services providers and users who merely transmit unlawful communications, or who engage in so-called good faith efforts to eliminate such material from their services:

Sec. 230. Protection for private blocking and screening of offensive material.

[*356] ...

(c) Protection for "Good Samaritan" Blocking and Screening of Offensive Material.

(1) Treatment of publisher or speaker.

No provider or user of interactive computer services 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 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).ⁿ⁴⁷

In 1998, in the wake of the Supreme Court's ruling that sections 223(a) and (d) of the Act were unconstitutional, Congress added a new section following the CDA's section 230. The new section 231, entitled, "Restriction of Access by Minors to Materials Commercially Distributed by Means of World Wide Web That Are Harmful to Minors," was the Senate-initiated attempt to rehabilitate the goals of then-defunct section 223(d)ⁿ⁴⁸ as it related to Internet ISPs. Following the requirement in subsection (a) that users of the World Wide Web take measures to restrict access by minors to "harmful material,"ⁿ⁴⁹ Congress reinforced the immunity of ISPs. The limited scope of subsection (a) is clarified in the succeeding section:

47 U.S.C. 231. Restriction of access by minors to materials commercially distributed by means of world wide web that

are harmful to minors

...

(b) Inapplicability of carriers and other service providers

For purposes of subsection (a), a person shall not be considered to make any communication for commercial purposes to the extent that such person is -

...

(3) a person engaged in the business of providing an Internet information location tool; or

[*357] (4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with subsection (c) or section 230 shall not constitute such selection or alteration of the content of the communication. ⁿ⁵⁰

Subsection (c), to which the previous section refers, provides:

(c) Affirmative Defense

(1) Defense

It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access to material that is harmful to minors -

...

(C) by any ... reasonable measures that are feasible under available technology.

(2) Protection for use of defenses.

No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this subsection or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section. ⁿ⁵¹

Like its predecessor, section 231 proved an ill-fated piece of legislation. On February 1, 1999, the District Court for the Eastern District of Pennsylvania permanently enjoined this revised attempt to regulate Internet content under the auspices of the First Amendment. ⁿ⁵² Thus, section 231 will meet the same fate as its legislative ancestor.

Nonetheless, the context in which the initial round of amendments to the CDA was adopted is worthy of study, as it provides insight into how Congress balanced policy. Lawmakers had to tackle the significant concern of offensive Internet material being accessible to children while making accommodation for the undeniable fact that service provider monitoring of each piece of material transmitted is an objective, technological impossibility. Add free speech concerns to the mix of policy considerations, and the fine line on which Congress was called upon to act becomes apparent.

Despite the judicial roadblocks and frustrations Congress has encountered along the way, the underlying policy has remained unchanged. Thus, while the public outcry concerning fraud in the online auction industry admittedly pales in

comparison to the depth of concern over the Internet's development as the most readily accessible and profitable forum for obscenity, one can fairly anticipate that the same types of policy arguments may be revisited by Congress when it is called upon to resolve the parallel issue of Internet fraud.ⁿ⁵³ Consumers can justifiably [*358] expect that the industry will argue that it is an objective, technological impossibility for online auction house personnel to read and verify every one of the huge number of transactions conducted daily, screening each customer-authored advertisement for indicia of fraud. Consumers also should be aware of the road chosen by Congress in the Communications Decency Act based on the policy arguments put forth by the service provider industry to provide immunity from and defenses to charges of otherwise unlawful acts of indecent or defamatory communications.

IV. An Examination of the Legislative History of Immunities and Defenses Advanced in the Communications Decency Act and the Online Family Empowerment Amendments

A. The Senate Proposal

Examining the legislative history surrounding the much-debated Telecommunications Act of 1996 is helpful for understanding the evolution of the CDA. Following months of extensive revisions and Senate Commerce Committee hearings on other provisions of the CDA, Senator Exon offered on the Senate floor only a small piece of this massive overhaul of the telecommunications industry.ⁿ⁵⁴ In particular, Senator Exon and Senator Coats jointly sponsored an amendment to the 1994 Communications Decency Act.ⁿ⁵⁵ Section 402, in the words of Senator Exon, was simply designed to ensure that the "laws which already apply to obscene, indecent, and harassing telephone use and the use of the mails should also apply to computer communications."ⁿ⁵⁶ Citing the fact that lewd materials are available in public spaces free of charge, his amendment sought to apportion enhanced criminal liability on the purveyors of offensive, indecent, or annoying material.ⁿ⁵⁷ As explained by Senator Coats:

Mr. President, all we are saying is, if you are in the business of providing this material, you have to provide barriers so it does not get in the hands of children. If you are an adult who wants to receive this material, you have to call up and get it. You have to subscribe to it. You have to prove you are an adult before you receive it.

...

We also require commercial on-line services to adopt this standard. If they wish to provide indecent material, they have to make what we call an effective, good-faith effort to segregate it from access to children ...ⁿ⁵⁸

Senator Exon explained that his amendment was designed as a law enforcement tool aimed at enhancing the ability of federal prosecutors to detect and punish those who distribute obscenity electronically, particularly those who distribute such [*359] material to children via computers.ⁿ⁵⁹ Accordingly, the vast majority of enforcement responsibility would rest with federal authorities, predominantly the Federal Communications Commission. The prohibitions in the Exon-Coats Amendment thus would be refined through extensive rulemaking.

As originally drafted, the Exon Amendment also would have exposed on-line ISPs, or mere conduits of information, to expanded criminal liability for the mere transmission of unlawful material. According to one commentary, the body of which was read into the Senate proceedings, the Senate proposal to curb offensive information on the Internet would force "the middlemen-on-line services in the United States to do the work of censorship, and that work is a practical impossibility."ⁿ⁶⁰

In response to an impressive, and by no means unexpected, flex of industry muscle,ⁿ⁶¹ an important refinement of Exon's original proposal was to insulate from liability what he called mere "mailmen" for computer messages,ⁿ⁶² later defined as online ISPs. In language that was particularly disturbing to the Justice Department,ⁿ⁶³ Senator Exon proposed that online ISPs and entities that maintain bulletin boards like Usenet be immune from liability for the

distribution of offensive or indecent material if they were mere conduits of the information and they lacked the ability to "control" the content of the postings. Additionally, "good faith" defenses were incorporated to ensure that an access provider, like Prodigy at the time, who took measures to control or reserved the right to edit content provided by third parties would no longer incur liability for restricting access to or distributing prohibited communications. ⁿ⁶⁴ In his clarification of the purpose of his amendment, Senator Coats remarked, "I wanted to clarify that it is the intent of this legislation that persons who are providing access to or connection with Internet or other electronic service not under their control are exempted under this legislation." ⁿ⁶⁵ Senator Exon reinforced this intent with the following:

[The amendment] explicitly exempts a person who merely provides access to or connection with a network like the Internet for the act of providing such access... An online service that is providing its customers with a gateway to networks like the Internet or the worldwide web over which it has no control is generally not aware of the contents of the communications which are being made on these networks, and therefore it should not be responsible for those communications. ⁿ⁶⁶

Whereupon, the following exchange ensued:

[*360]

Mr. COATS. I understand that in a recent New York State decision, *Stratton Oakmont versus Prodigy* [referencing *Stratton Oakmont, Inc. v. Prodigy Services Co.* ⁿ⁶⁷], the court held that an online provider who screened for obscenities was exerting editorial content control. This led the court to treat the online provider as a publisher, not simply a distributor, and to therefore hold the provider responsible for defamatory statements made by others on the system. I want to be sure that the intend [sic] of the amendment is not to hold a company who tries to prevent obscene or indecent material under this section from being held liable as a publisher for defamatory statements for which they would not otherwise have been liable.

Mr. EXON. Yes; that is the intent of the amendment.

Mr. COATS. And am I further correct that the ... defense is intended to protect companies from being put in such a catch-22 position? If they try to comply with this section by preventing or removing objectionable material, we don't intend that a court could hold that this is assertion of editorial content control, such that the company must be treated under the high standard of a publisher for the purposes of offenses such as libel.

Mr. EXON. Yes; that is the intent of [the] section.

...

Mr. HELMS. Mr. President, I would inquire of the Senator from Indiana if my understanding is correct that, under ... your amendment, a person is protected solely for providing access. Is that correct?

Mr. COATS. The Senator is correct, this is a narrow defense. The defense is for solely providing access or connection and not a defense for any person or entity that provides anything more than solely providing access. This does not create a defense for someone who has some level of control over the material or the provision of material ... This defense does not apply to someone who, among other things, manages the prohibited ... material, charges a fee for such material, provides instructions on how to access such material, or provides an index of the material. This is merely an illustrative list and not an exhaustive list of the types of activities that would qualify as solely providing access of connection ... ⁿ⁶⁸

Significantly, although the Senate debate was replete with references to the effect that the Exon-Coats Amendment was

intended to insulate ISPs from broad-based tort liability for common law torts like defamation, the Conference Committee clearly curtailed this far-reaching conclusion. In particular, the Conference Committee explained that the purpose of the Exon-Coats defenses was to ensure:

Commercial and non-profit Internet operators who provide access to the Internet and other interactive computer services shall not be liable for indecent material accessed by means of their services. This provision is designed to target the criminal penalties of new sections 223(a) and (d) at content providers who violate this section and persons who conspire with such content providers, rather than entities that simply offer general [*361] access to the Internet and other online content. The conferees intend that this defense be construed broadly to avoid impairing the growth of online communications through a regime of vicarious liability. ⁿ⁶⁹

As discussed more fully later in this article, the Conference Committee narrowly interpreted the amendment to apply only to criminal prosecutions authorized by new section 223(d). ⁿ⁷⁰ Thus, the Conference Committee's interpretation most likely contributed to its decision to adopt significant portions of what were initially described by their sponsors as mutually exclusive House and Senate approaches to the online pornography problem in the final reported bill.

The Senate's decision to insulate ISPs from liability was also attributed to the practical impossibility of holding mere access providers responsible for the millions of pieces of information they receive and transmit each day. As James Gleick noted in his article *This Is Sex?*, ⁿ⁷¹ "forcing the middlemen-on-line services in the United States to do the work of censorship ... is a practical impossibility." Senator Leahy reinforced this unfathomable task of censorship in his comments wherein he noted, "A typical Internet provider carries more than 10,000 groups. As many as 100 million new words go through them every day. Are we going to have a whole new group in the Justice Department checking these 100 million new words to find out if they are wrong?" ⁿ⁷²

Finally, the debate was fraught with references to the congressional desire to minimize government interference with new technology that had blossomed by virtue of the fact that it was not stifled, restricted or regulated. ⁿ⁷³ As Senator Feingold noted in his remarks in support of the Leahy study alternative, ⁿ⁷⁴ the Exon-Coats Amendment would have the "potential to retard significantly the development of this new type of interactive telecommunications." ⁿ⁷⁵ Senator Feingold continued, "Whenever there is a choice between Government intervention and empowering people to make their own decisions, we ought to try first to use the situation ... that involves less Government control of our lives." ⁿ⁷⁶ And, in reference to the Exon-Coats Amendment, Senator Leahy stated, "We should avoid quick fixes today that would interrupt and limit the rapid evolution of electronic information systems - for the public benefit far exceeds the problems it invariable creates by the force of its momentum." ⁿ⁷⁷

In the final analysis, Senate Bill 652 created new defenses to assure that the mere provision of access to an interactive computer service or good faith monitoring or filtering of content did not create liability. ⁿ⁷⁸ The debate on the amendment clarifies that it was intended to insulate ISPs from liability via immunity or defenses based [*362] on an ISP's decision either to restrict third party access to "offensive" material, or to engage in technological "censoring" of constitutionally protected content.

Despite the bipartisan sponsorship of his amendment and the fact that virtually no other lawmaker contested the goal of protecting the innocence of the nation's children, Senator Exon's proposed enforcement methods drew fire. In particular, Senator Leahy cited grave concerns about chilling the development of and entry into cyberspace. ⁿ⁷⁹ He proposed the alternative of an intensive five-month study by the Attorney General and the National Telecommunications Information Administration into the best ways to minimize the accessibility of pornography in the least offensive way, vis-a-vis, the First Amendment's free speech guarantee. ⁿ⁸⁰

B. The House Proposal

Meanwhile, the House of Representative was intent upon the business of developing its own comprehensive telecommunications bill, H.R. 1555, introduced May 3, 1995 by Representative Thomas Bliley. ⁿ⁸¹ There was virtually no House equivalent to the Exon-Coats proposal. Fundamentally, the House strategy for curbing lewd and offensive material in cyberspace contained a different emphasis. In particular, Representatives Cox and Wyden introduced an amendment that embodied the House approach known as the "Online Family Empowerment" Amendment as an alternative to the Exon-Coats proposal. ⁿ⁸² In explaining their alternative of promoting technological, end-user controls to minimize offensive communications, Representative Cox stated:

Some have suggested, Mr. Chairman, that we take the Federal Communications Commission and turn it into the Federal Computer Commission, that we hire even more bureaucrats and more regulators who will attempt, either civilly or criminally, to punish people by catching them in the act of putting something into cyberspace.

Frankly, there is just too much going on on the Internet for that to be effective. No matter how big the army of bureaucrats, it is not going to protect my kids because I do not think the Federal Government will get there in time. ⁿ⁸³

Sentiments that legislation should ultimately bolster the ability of ISPs and parents/consumers to screen or filter at the receiving end through new technologies rather than to simply give the government additional enforcement tools to punish [*363] those who initiate or transmit offensive material were reinforced by the amendment's co-sponsor, Representative Wyden.

Now what the gentleman from California [Mr. Cox] and I have proposed does stand in sharp contrast to the work of the other body. They seek there to try to put in place the Government rather than the private sector about this task of trying to define indecent communications and protecting our kids. In my view that approach, the approach of the other body, will essentially involve the Federal Government spending vast sums of money trying to define elusive terms that are going to lead to a flood of legal challenges while our kids are unprotected. The fact of the matter is that the Internet operates worldwide, and not even a Federal Internet censorship army would give our Government the power to keep offensive material out of the hands of children who use the new interactive media, and I would say to my colleagues that, if there is this kind of Federal Internet censorship army that somehow the other body seems to favor, it is going to make the Keystone Cops look like crackerjack crime-fighter [sic]. ⁿ⁸⁴

With regard to the enlistment of ISPs in the legislative assault on an industry that was frequently characterized as one that destroys the innocence of children, Representative Cox further noted:

Ironically, the existing legal system provides a massive disincentive for the people who might best help us control the Internet to do so.

I will give you two quick examples: A Federal court in New York, in a case involving CompuServe, one of our on-line service providers, held that CompuServe would not be liable in a defamation case because it was not the publisher or editor of the material. It just let everything come onto your computer without, in any way, trying to screen it or control it.

But another New York court, the New York Supreme Court, held that Prodigy, CompuServe's competitor, could be held liable in a \$ 200 million defamation case because someone had posted on one of their bulletin boards, a financial bulletin board, some remarks that apparently were untrue about an investment bank, that the investment bank would go out of business and was run by crooks.

Prodigy said, "No, no; just like CompuServe, we did not control or edit that information, nor could we, frankly. We have over 60,000 of these messages each day, we have over 2 million subscribers, and so you cannot proceed with this kind of a case against us."

The court said, "No, no, no, no, you are different; you are different than CompuServe because you are a family-friendly network. You advertise yourself as such. You employ screening and blocking software that keeps obscenity off of your network. You have people who are hired to exercise an emergency delete function to keep that kind of material away from your subscribers. You don't permit nudity on your system. You have content guidelines. You, therefore, are going to face higher, stricter [sic] liability because you tried to exercise some control over offensive material."

[*364] Mr. Chairman, that is backward. We want to encourage people like Prodigy, like CompuServe, like America Online, like the new Microsoft network, to do everything possible for us, the customer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see ...

We can go much further, Mr. Chairman, than block obscenity or indecency, whatever that means in its loose interpretations. We can keep away from our children things not only prohibited by law, but prohibited by parents. That is where we should be headed, and that is what the gentleman from Oregon [Mr. Wyden] and I are doing. ⁿ⁸⁵

Notably, Senator Feingold's remarks supporting the Leahy study during the Senate floor debate, similarly noted that provider and end-user technological solutions are preferable to government regulation that may interfere with free speech, wherein he stated, "the opportunity exists to solve at least part of the problem through the marketplace today, not through governmental prohibitions... None of the technical safeguards available, such as blocking software and provider screening, are perfect, but the nice thing is they do not violate the first amendment." ⁿ⁸⁶

Policy considerations on the House side were consistent with those articulated in the Senate. In fact, one of the stated policies of the Online Family Empowerment enactment provides:

(b) POLICY. - It is the policy of the United States to -

(2) Preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by State or Federal regulation. ⁿ⁸⁷

In succeeding subsection (c), the text of the Cox amendment provided as follows:

"(c) PROTECTION FOR 'GOOD SAMARITAN' BLOCKING AND SCREENING OF OFFENSIVE MATERIAL. - No provider or user of interactive computer services shall be treated as the publisher or speaker of any information provided by an information content provider. No provider or user of interactive computer services shall be held liable on account of -

(1) any action voluntarily taken in good faith to restrict access to 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

(2) any action taken to make available to information content providers or others the technical means to restrict access to material described in paragraph (1). ⁿ⁸⁸

Thus, regardless of the fundamental differences in what policies should be emphasized in the offensive and indecent

Internet communications battle [*365] ("topdown" model of government regulation versus end-user control), both houses clearly recognized the need to enlist the so-called middleman ISPs, and to provide immunity from liability for (1) ISPs who merely transmit indecent information provided by third parties, and (2) ISPs who engage in good faith efforts to monitor or restrict information received from third parties or who develop and market filtering or screening technology.

C. The Conference Committee Report

When Senate Bill 652 was transmitted to the House of Representatives, the House deleted the Senate provisions, and substituted the language of House Bill 1555, ⁿ⁸⁹ which included the Cox-Wyden language. ⁿ⁹⁰ The legislation was then submitted to a number of conference committees.

Following joint consideration by members of the House and Senate, the Conference Committee advocated the adoption of both the House and Senate amendments. The Cox-Wyden Amendment, with minor technical modifications, ⁿ⁹¹ was codified in new section 230 of the Communications Decency Act. This ensured that ISPs who took steps to monitor, edit or refuse to carry certain content were not subject to civil liability for their actions, like that endured by Prodigy in the previously-cited defamation case. ⁿ⁹² The Exon-Coats proposal, which was originally characterized as an alternative to the Cox-Wyden Amendment, was also adopted. This preserved the defense to criminal prosecution or government-assessed civil penalties under the foregoing sections of section 223 that "protects entities from liability for providing access or connection to or from a facility, network or system not under their control. The defense covers [the] provision of related capabilities incidental to providing access, such as server and software functions, that do not in involve the creation of content." ⁿ⁹³ "Good faith" efforts like those undertaken by Prodigy were specifically rewarded by extending immunity to those ISPs who made efforts to verify content or control access to unlawful material. As the conferees reported in describing the scope of language that is currently codified as 47 U.S.C. 223(e)(6): "A good faith defense is provided for 'reasonable, effective, and appropriate' measures to restrict access to prohibited communications. The word 'effective' is given its common meaning and does not require an absolute 100 percent restriction of access to be judged 'effective.'" ⁿ⁹⁴

If interactive computer ISPs and users are immune from civil and criminal liability for content, whether they elect to pass along information indiscriminately or engage in effective measures to screen out objectionable material, it stands to reason that the same policies underlying congressional action would hold true for online auction services.

[*366] First, holding auctioneers responsible for fraudulent content might have a chilling effect on constitutionally protected commercial speech, particularly where it is clear that Congress does not wish to unnecessarily tether Internet development. Second, the objective impossibility of effectively monitoring the millions of pieces of information processed each day by these cyberspace auctioneers would mitigate against liability for the fraudulent postings and activities of third party information suppliers. If Congress does choose to offer immunity to commercial online auctions, what price should the law exact? In light of congressional debate, it is at least arguable that the services currently offered by eBay (insurance, feedback forums, and escrow) "effectively" counter the imposition of liability as that term is embraced in the current version of 47 U.S.C. 223(e)(6).

To date, the courts have done little to provide meaningful remedies for online victims, or suggest policy alternatives. In fact, there is a trend among the courts to liberally construe the provisions of the CDA, at least suggesting that ISPs should be immunized for tort-based liability generally in the interest of preserving the vitality of the Internet.

V. Judicial Interpretation of Section 230 of the Communications Decency Act

Before embarking on a discussion of judicial decisions, it is notable that several online auctions provide feedback forums, known as "feedback" in eBay's case. This site allows buyers to post generally accessible messages about their dealings with sellers and their assessment of merchandise and pricing. Thus, eBay invites user comment/notification about problems encountered through use of their service. Judicial policy addresses these types of online "monitoring"

efforts and their impact on section 230 immunity in the case of *Zeran v. America Online, Inc.* ⁿ⁹⁵

On April 25, 1995, in the aftermath of the Oklahoma City bombing of the Murrah Building, Kenneth Zeran (Zeran) found himself the victim of a malicious hoax perpetrated via the Internet services of America Online, Inc. (AOL). Specifically, an unknown person or persons, acting without Zeran's knowledge or approval, affixed Zeran's name and telephone number on a series of notices on AOL's electronic bulletin board advertising t-shirts and other items glorifying the bombing. As might be expected, Zeran received numerous disturbing and threatening telephone calls, including death threats, from people who were outraged with the posted notices. When Zeran notified an AOL representative that he was not affiliated with the authors of the notices and demanded that the information be removed, AOL complied, and ultimately agreed to terminate the account from which the messages emanated. However, as a matter of company policy, the representative refused to post a retraction of the original notice. Nonetheless, the same day AOL removed the original notices, slightly altered notices reappeared. ⁿ⁹⁶

For business reasons, Zeran was not willing to change his telephone number. Consequently, during the latter days of April 1995, he received a threatening or [*367] abusive telephone call approximately every two minutes, ⁿ⁹⁷ causing the police to place him under protective surveillance. After extensive publicity efforts to expose the hoax, the calls eventually dwindled to fifteen per day by mid-May 1995. ⁿ⁹⁸

Zeran filed a complaint against AOL, alleging that it had been negligent in failing to respond adequately to notification of the bogus postings. ⁿ⁹⁹ AOL countered with a Federal Rule of Civil Procedure 12(b)(6) motion, alleging that the state defamation action was preempted by section 230 of the Communications Decency Act. ⁿ¹⁰⁰

The trial court dismissed the defamation claim based on section 230, stating in defense of Congress' decision to relieve ISPs of tort liability:

Internet providers subjected to distributor liability are less likely to undertake any editing or blocking efforts because such efforts can provide the basis for liability ... Similarly, an Internet provider maintaining a hot-line or other procedure by which subscribers might report objectionable content in the provider's interactive computer system would expose itself to actual knowledge of the defamatory nature of certain postings and, thereby, expose itself to liability should the posting remain or reappear. Of course, ... a [sic] Internet provider can easily escape liability on this basis by refraining from blocking or reviewing any online content... Clearly, then, distributor liability discourages Internet providers from engaging in efforts to review online content and delete objectionable material, precisely the effort Congress sought to promote in enacting the CDA. ⁿ¹⁰¹

On appeal, the decision of the district court was affirmed. ⁿ¹⁰² In affirming the lower court's decision under the preemption doctrine, the circuit court concluded:

Congress' purpose in providing the 230 immunity was thus evident. Interactive computer services have millions of users. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for [Internet] service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer [Internet] service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize [Internet] service providers to avoid any such restrictive effect. ⁿ¹⁰³

In response to Zeran's argument that notifying AOL the postings were defamatory and harmful removed it from the protections of section 230, the court stated:

[*368]

Zeran next contends that interpreting 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes ... Zerán fails, however, to understand the practical implications of notice liability in the interactive computer service context...

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement - from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability ... Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages ... Thus, ... liability upon notice has a chilling effect on the freedom of Internet speech. ⁿ¹⁰⁴

Of concern, the court seemed impressed with the fact that it was not interpreting the law in a manner that would deny Zerán a traditional avenue of recovery. The court stated:

None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability. While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer. ⁿ¹⁰⁵

In light of the difficulty with identification on the Internet, however, this remedy may mean little to a defrauded e-consumer.

Of greater concern is the court's loosely-worded conclusion that hints at the need to absolve ISPs of all tort-based liability. "The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits would pose to freedom of speech in the new and burgeoning Internet medium." ⁿ¹⁰⁶ Thereafter, following broad references to congressional intent to refrain from unduly regulating a new, beneficial medium as evidenced in the "Findings" ⁿ¹⁰⁷ and "Policy" ⁿ¹⁰⁸ provisions that precede section 230(c), ⁿ¹⁰⁹ the court stated:

Congress made a policy choice, ... not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.

[*369]

Congress' purpose in providing the 230 immunity was thus evident. Interactive computer services have millions of users. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for [Internet] service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize [Internet] service providers to avoid any such restrictive effect. ⁿ¹¹⁰

The exclusive availability of the legally frail remedy of a common law action against the unknown perpetrator of defamatory material was reiterated verbatim in *Blumenthal v. Drudge & America Online, Inc.* ⁿ¹¹¹ In that

well-publicized case, Sydney Blumenthal and his wife initiated an action against AOL and Matthew Drudge, the publisher of an AOL-sponsored newsletter, for allegedly defamatory statements made in the so-called, "Drudge Report."ⁿ¹¹² The Blumenthal court denied recovery to the plaintiffs against AOL despite its repeated references to the elusiveness of the true culprit in online defamation cases. "To paraphrase Gertrude Stein, as far as the Internet is concerned, not only is there perhaps 'no there there,' the 'there' is everywhere there is Internet access."ⁿ¹¹³ In Blumenthal, however, the identity of the alleged defamer was known from the inception of the litigation, as it was the perpetrator's "Drudge Report" that contained the statements at issue.ⁿ¹¹⁴ This perhaps made it an easier case to dismiss AOL's potential liability.

More importantly, in an apparent attempt to set the stage for making regulatory distinctions between the Internet and other forms of mass communication, the court declared:

"The Internet is fundamentally different from traditional forms of mass communication in a least three important respects. First, the Internet is capable of maintaining an unlimited number of information sources ... Second, the Internet has no "gatekeepers" - no publishers or editors controlling the distribution of information... Finally, the users of Internet information are also its producers. But every person who taps into the Internet is his [or her] own journalist. In other words, the Internet has shifted the focus of mass communication to the individual"ⁿ¹¹⁵

Through this discussion, it is apparent that the court is paving the way for sharp distinctions between the Internet and traditional forms of communication that may mitigate against the imposition of tort liability beyond that embodied in section 230. [*370] In fact, the language of the Blumenthal decision indicates that a broader insulation beyond defamation is possible:

Whether wisely or not, it [Congress] made the legislative judgment to effectively immunize providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others. In recognition of the speed with which information may be disseminated and the near impossibility of regulating information content, Congress decided not to treat providers of interactive computer services like other information providers such as newspaper, magazines or television and radio stations, all of which may be held liable for publishing or distributing obscene or defamatory material written or prepared by others. While Congress could have made a different policy choice, it opted not to hold interactive computer services liable for their failure to edit ... material disseminated through their medium.ⁿ¹¹⁶

From this limited sampling of decisions, one may conclude that courts have interpreted section 230 with rationales which parallel congressional decision-making. There is a readiness to acknowledge directly the same issues of impossibility of monitoring that would apply to online auction houses, interactive services that maintain and provide access to millions of advertisement and bid solicitations each day. Notably, the courts seem willing to interpret section 230 in ways which surpass congressional intent, and have clearly indicated that the Internet should not be subject to the same responsibilities imposed on more traditional common law tort defendants.

If, as in the case of the CDA, Congress is reticent about regulation that might curtail the growth of the Internet medium, it may conclude that mandatory monitoring for fraud is not an economically or technologically feasible alternative. If monitoring is not mandated, it is likely that efforts by online auctioneers to provide nominal insurance, feedback forums, and the like will stand in place of "effective, good faith" measures to detect fraudulent material that Congress deemed adequate to invoke ISP immunity in section 231.

VI. Conclusion

As mentioned at the outset, Internet fraud is not insignificant. In fact, there is some suggestion that it is on the rise. The growing popularity of Internet "auction houses" further suggests that, while maybe not as insidious as Internet pornography, manipulations of the media may rise to destructive levels.

It is not surprising that auction houses have attempted to limit their liability through contract. This pattern is no different from the normal merchant or auction house. To the extent similar, application of traditional commercial liability should be no different. Reasonable limitations should thus be permissible.

Where a non-cyber auctioneer could likely be held liable for participating in fraud, however, e-commerce auction houses point to the obvious differences in their means and volume of conducting business. In addition, where policy suggests that [*371] the facilitator of the transactions should participate in allocation of the risk of loss, e-commerce houses likewise point to the impossibility of effective overview.

E-commerce, particularly with auction houses, presents a new set of problems to address. The sheer volume is staggering. No earth-bound auction house could dare participate in as many transactions. Similarly, as with economic development early in U.S. history, there is a preference to practice a form of laissez-faire so as not to inhibit growth of the emerging cyber economy.

The approach taken by Congress in addressing ISP facilitation of pornography provides one example of a likely approach regulators may apply when the issue of cyber fraud reaches proportions requiring some action. Congress had several reasons for immunizing ISPs in section 230: concern about appropriate constitutional protection of speech, a recognition of the impossibility of effective enforcement because of volume and cost, and the reluctance to stifle an amazing new form of doing business. In so acting, Congress chose to allocate risk in favor of preserving the system and away from protecting individual participants. This approach will likely reappear to form some regulative control over cyber business. Once again, regulation will seek to preserve the system at the peril of the individual participants.

There are some differences warranting mention that may suggest congressional departure from the avenue chosen in sections 223 and 230 of the CDA. First, the vigor with which legislative action might be applied to online fraud could be considerably different. As the reader will recall, commercial speech is protected at a substantially lesser level than section 230 related speech. This means that Congress may be more inclined to act without concern for the level of its involvement. This also may signal that more regulation could be possible.

Nonetheless, Congress will likely defer to the established model. Unfortunately, that will put many consumers at risk to incur loss not likely to be recovered. While deference to industry growth and minimization of government involvement in business has a nice ring, it may in the long term be more destructive. In the alternative, ordered growth at the outset may be a better route. Balancing of risks and allocation of loss now may assure reasonable growth and expansion with optimum protection of all involved.

Volume and difficulty with review of content has not always served as a convincing argument resulting in non-regulation. The classic example is the check processing industry where drawees, such as banks, act as "third persons" in the process of transferring funds from the drawer to the payee. In appearance, the drawee is not unlike the ISP, acting merely as the conduit of the transfer of funds. Drawees, however, have long borne some or all of the risk of loss, ostensibly because they receive economic benefit for their participation. The banking industry long recognized that it could not examine every item presented for collection in the system. Consequently, it assumed risk of loss within the system and developed its own set of internal rules designed to control its risk. This may present an alternative model to create a structure for controlling risk in the whole system.

Society may be best served with minimal government regulation of cyber business so that the industry has the opportunity to develop to a fuller potential. Should Congress or another regulator follow the model discussed in the body of this paper, the following suggestions may be useful.

[*372] First, one startling aspect of Zeran was Zeran's assertion that obtaining identification of the true tortfeasor

was "made ... impossible [by AOL's] failing to maintain adequate records of its users." ⁿ¹¹⁷ Discovery of the true identity was precluded by AOL's membership practices. While it maintains the names, addresses, phone numbers, and credit card numbers of its members, it does not verify such information for a "trial membership." In this case, the wrongdoer utilized the trial membership to open not one but three accounts in succession with false information. ⁿ¹¹⁸ Given the court's deference to Zeran's private tort remedy, it is shocking that one can purposefully engage in tortious behavior and avoid discovery, simply by providing false information to an ISP such as AOL. In this case, this particular person did so three consecutive times. ⁿ¹¹⁹

It might be suggested that this is an isolated incident, and ISPs should not be burdened with identity verification prior to allowing use of their services. Nevertheless, AOL's membership recordkeeping facilitated this incident and easily could do so for many more. At present there appears to be no balance between the potential for harm and the means to provide an avenue of remedy. That ISPs should develop a means to assist in the identification of system users, at least to the extent that verifiable information be obtained prior to allowing a user online. While no mention is made of an attempt to trace the user through computer "signatures" as has been done to identify creators of viruses, ISPs ought to maintain at least this information.

This should apply to ISPs and any other cyber business, whether dealing direct or through an auction like process. Such businesses should be required to establish and maintain accurate records, using reasonable means to acquire correct information, or at least reasonable means to trace identity, of users for a period of time necessary to assure availability within appropriate statutes of limitations, for example, four years under U.C.C. section 2-725. Sufficient sanction should be imposed to encourage storage of potentially significant records.

Second, attempts to mollify cyber auction traders with "insurance" up to some nominal amount fails to provide adequate protection. One, more adequate, possibility would be to require cyber business traders, for example, auction houses, to offer insurance to the value of the transaction at a reasonable price.

In closing, cyber business presents a familiar conflict of unfettered growth versus growth limited by transaction-inhibiting regulation. Congress has suggested its likely path when regulation of business activities over the Internet becomes an issue before it. There may be, however, some differences that warrant different treatment. In the end, its methods should provide a balancing of the appropriate risks and benefits in the interests of all participants.

Legal Topics:

For related research and practice materials, see the following legal topics:

Computer & Internet Law
 Censorship
 General Overview
 Computer & Internet Law
 Criminal Offenses
 Data Crimes & Fraud
 Computer & Internet Law
 Internet Business
 General Overview

FOOTNOTES:

n1. See Ken Bensinger, *The Perils of Online Auctions*, Wall St. J., Mar. 5, 1999, at W1.

n2. eBay is the world's largest online trading community, and a pioneer in person-to-person online trading. Founded in 1995, eBay has developed an auction format on the Web that is available 24 hours a day, 7 days a week. eBay has more than 1 million registered users. As of April 16, eBay reported having 800,000 items listed for sale, with more than 100,000 items added daily in over a thousand categories. See *eBay Soars to New Heights: 1-29-00* (visited Aug. 29, 2000) <<http://pages.ebay.com/community/aboutebay/releases/9901.html>> [hereinafter

eBay Soars].

n3. See Rob Turner, *Winning Bid: The Hot Web Auction Site eBay*, *Money*, Mar. 1999, at 201.

n4. See Bensinger, *supra* note 1, at W1.

n5. See Roger Taylor, *Web Auction Sites Face Fraud Inquiry*, *London Fin. Times*, Jan. 27, 1999, at 13.

n6. See eBay, *Auction Sites Subject of Fraud Investigation*, *S.F. Chron.*, Jan. 26, 1999, at C1. See also eBay Investigations (visited Aug. 16, 2000) <<http://pages.ebay.com/help/community/investigates.html>> (noting current fraud policy).

n7. See SafeHarbor Insurance Overview (visited Jan. 7, 2000) <<http://pages.ebay.com/services/safeharbor/safeharbor-insurance.html>>.

n8. eBay Soars, *supra* note 2.

n9. See *id.*

n10. See *id.*

n11. See Andrea Petersen, *Commerce Initiative Is Set by Top Executives at 17 Companies*, *Wall St. J.*, Jan. 15, 1999, at B6.

n12. *Id.* (quoting David Banisar, policy director of the Electronic Privacy Information Center, a Washington, D.C. advocacy group).

n13. Communications Decency Act of 1996, Pub. L. No. 104-104, 501, 110 Stat. 133 (1996) (codified as amended at 47 U.S.C. 201-276 (1998)).

n14. 47 U.S.C. 230 (1998).

n15. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended at 47 U.S.C. 201-276 (1998)).

n16. See *eBay Soars*, *supra* note 2.

n17. Compare *supra* note 13, with *supra* note 15.

n18. See 47 U.S.C. 223(a) (1998).

n19. As noted by the Supreme Court in *Reno v. ACLU*: "An e-mail address provides no authoritative information about the addressee, who may use an e-mail 'alias' or an anonymous remailer. There is also no universal or reliable listing of e-mail addresses and corresponding names and telephone numbers, and any such listing would be or rapidly become incomplete." 521 U.S. 844, 855 n.20 (1997).

n20. 47 U.S.C. 223, 230 (1998).

n21. As an aside, volume and difficulty with review of content has not always served as a convincing argument resulting in non-regulation. The classic example is the check processing industry where drawees such as banks act as "third persons" in the process of transferring funds from the drawer to the payee. In appearance, the drawee is not unlike the ISP, acting merely as the conduit of the transfer of funds. Drawees,

however, have long born some or all of the risk of loss, ostensibly because they receive economic benefit for their participation. The banking industry long recognized that it could not examine every item presented for collection in the system. Consequently, it has assumed risk of loss within the system and developed its own set of internal rules designed to control its risk. This may present an alternative model to create a structure for controlling risk in the whole system, as discussed in this article's conclusion.

n22. eBay User Agreement Item Nos. 3.-3.2 (visited Jan. 7, 2000) <<http://pages.ebay.com/help/community/png-user.html>> [hereinafter eBay User Agreement].

n23. *Id.* at Item No. 3.3 (emphasis added).

n24. *Id.* at Item Nos. 6, 6.1.

n25. *Id.* at Item No. 12.

n26. See Bensinger, *supra* note 1, at W1.

n27. See Turner, *supra* note 3, at 201.

n28. See Taylor, *supra* note 5, at 13.

n29. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 61 (1996) (codified as amended at 47 U.S.C. 201-276 (1998)).

n30. S. Rep. No. 104-230, at 1 (1996).

n31. See generally Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 61 (1996) (referring to tits. I-II, IV-VII) (codified as amended at 47 U.S.C. 151 (1998)).

n32. See generally 141 Cong. Rec. S7881 (1995); 141 Cong. Rec. S7942 (1995); 141 Cong. Rec. S8055 (1995); 141 Cong. Rec. S8134 (1995); 141 Cong. Rec. S8206 (1995); 141 Cong. Rec. S8305 (1995); 141 Cong. Rec. S8417 (1995); 141 Cong. Rec. H8269 (1995); 141 Cong. Rec. H8425 (1995); 141 Cong. Rec. H9954 (1995); 141 Cong. Rec. S15144 (1995); 142 Cong. Rec. H1079 (1996); 142 Cong. Rec. H1145 (1996); 142 Cong. Rec. S686 (1996); H.R. Rep. No. 104-458 (1996), S. Rep. No. 104-230 (1996).

n33. Communication Decency Act of 1996, Pub. L. No. 104-104, 501, 110 Stat. 133 (1996) (codified as amended at 47 U.S.C. 223 (1998)).

n34. *Reno v. ACLU*, 521 U.S. 844, 858 n.24 (1997) (citing *Cyberporn and Children: The Scope of the Problem, The State of the Technology, and the Need for Congressional Action: Hearing on S. 692 Before the Senate Comm. on the Judiciary, 104th Cong. 7-8 (1995)* (statement of Sen. Patrick Leahy)).

n35. See 142 Cong. Rec. S6130 (1996); 142 Cong. Rec. S3146 (1996); 142 Cong. Rec. S2095 (1996); 142 Cong. Rec. S1646 (1996).

n36. See *Sable Communications of Cal., Inc. v. FCC*, 492 U.S. 115, 131 (1989).

n37. See 47 U.S.C. 223(b)-(c) (1998).

n38. See *Sable Communications*, 492 U.S. at 121-24.

n39. 141 Cong. Rec. S8310, S8345-46 (1995).

n40. See *Reno*, 521 U.S. at 870.

n41. *Id.* at 874, 877-78.

n42. Communications Decency Act Amendments of 1998, Pub. L. No. 105-277, 112 Stat. 2681-739.

n43. See *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999).

n44. 47 U.S.C. 223(e)(1) (1998).

n45. 47 U.S.C. 223(e)(5).

n46. 47 U.S.C. 223(e)(6).

n47. 47 U.S.C. 230(c) (1998).

n48. 47 U.S.C. 231(a) (1998). Section 223 survived the constitutional challenge largely unscathed due to the severability provisions of the Telecommunications Act. 47 U.S.C. 608 (1998). In short, the Supreme Court elected to sever the constitutionally offensive reference to "indecent" communications, leaving the sweeping prohibition against "obscene" communications intact. See *Reno v. ACLU*, 521 U.S. 844, 882 (1997).

n49. Thus, in enacting 47 U.S.C. section 230, Congress had abandoned its characterization of prohibited material as "patently offensive," electing to criminalize the provision of "material harmful to minors" to cure the prior version's constitutional shortcomings. It chose this avenue despite the Conference Committee's express rejection of the terms in its report wherein it originally adopted the Exon-Coats proposal. See 142 Cong. Rec. H1078, H1129-30 (1996).

n50. 47 U.S.C. 231(a)-(b) (1998).

n51. 47 U.S.C. 231(c).

n52. See *Reno*, 31 F. Supp. 2d at 499.

n53. See *Alleged Drug Sale on eBay Raises Liability Issue*, Wall St. J., May 30, 2000, at B18.

n54. Due to the fact that the amendment originated on the Senate floor, there is no legislative record of committee hearings and testimony that can account for the manner in which the language evolved.

n55. See 141 Cong. Rec. S8310 (1995).

n56. 141 Cong. Rec. S8329-30 (1995).

n57. See 141 Cong. Rec. S8329 (1995).

n58. 141 Cong. Rec. S8333 (1995).

n59. See 141 Cong. Rec. S8330 (1995).

n60. James Gleick, *This Is Sex?*, N.Y. Times, June 11, 1995, 6 (magazine), at 26.

n61. See 141 Cong. Rec. S8310, S8331 (1995).

n62. See 141 Cong. Rec. S8310, S8330 (1995).

n63. As pointed out by Acting Assistant Attorney General Kent Markus, the result of the language was to immunize online ISPs from liability if they did not control content, even if they had actual knowledge of the obscene or pornographic nature of materials posted on their sites. See 141 Cong. Rec. S8343 (1995) (letter of Kent Markus).

n64. See 142 Cong. Rec. H1078, H1099 (1996).

n65. 141 Cong. Rec. S8310, S8345 (1995).

n66. 141 Cong. Rec. S8310, S8345 (1995).

n67. No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at 1 (N.Y. Sup. Ct. May 24, 1995). See *infra* note 92 and accompanying text.

n68. 141 Cong. Rec. S8310, S8345 (1995).

n69. 142 Cong. Rec. H1078, H1129 (1996).

n70. 142 Cong. Rec. H1078, H1129 (1996).

n71. Gleick, *supra* 60, at 26.

n72. 141 Cong. Rec. S8310, S8332 (1995).

n73. See 141 Cong. Rec. S8330 (1995).

n74. See *infra* text accompanying note 86.

n75. 141 Cong. Rec. S8310, S8334 (1995).

n76. 142 Cong. Rec. S8336 (1995).

n77. 141 Cong. Rec. S8341 (1995).

n78. See generally 141 Cong. Rec. S8310 (1995).

n79. See 141 Cong. Rec. S8330 (1995).

n80. Although not adopted at the time of enactment of the CDA, it is not surprising that the crux of Senator Leahy's proposal was adopted in the 1998 amendments to the CDA that occurred in the wake of the successful constitutional challenge in *Reno v. ACLU*. See *supra* note 34. See also Communications Decency Act Amendments of 1998, Pub. L. No. 105-277, 112 Stat. 2681-2739 (study by Commission on Online Child Protection).

n81. See 141 Cong. Rec. H4520, H4545 (1995).

n82. Upon review of the Act, the authors believe that despite the characterization of Cox-Wyden as an alternative to Exon-Coats, both amendments were concurrently codified in the Act. See 142 Cong. Rec. H1145 (1996); 142 Cong. Rec. S721 (1996).

n83. 141 Cong. Rec. H8460, H8469 (1995).

n84. 141 Cong. Rec. H8470 (1995).

n85. 141 Cong. Rec. H8469-70 (1995).

n86. 141 Cong. Rec. S8310, S8336 (1995).

n87. 141 Cong. Rec. H8460, H8469 (1995).

n88. 141 Cong. Rec. H8460, H8469 (1995).

n89. See 141 Cong. Rec. H9954, H9999 (1995).

n90. The inclusion of the terms "or user" appeared for the first time on the floor of the House and carries with it no legislative record for the reason Congress determined to insulate "users" as well as "providers" of online services. See 141 Cong. Rec. H8460, H8471-72 (1995).

n91. See 142 Cong. Rec. H1078, H1130 (1996).

n92. See, e.g., *supra* note 67.

n93. 142 Cong. Rec. H1078, H1129 (1996).

n94. 142 Cong. Rec. H1128 (1996).

n95. 129 F.3d 327, 331 (4th Cir. 1997).

n96. See *id.* at 329.

n97. See id.

n98. See id.

n99. See id.

n100. See id.

n101. *Zeran v. America Online, Inc.*, 958 F. Supp. 1124, 1135 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997).

n102. See *Zeran*, 129 F.3d at 327.

n103. *Id.* at 331 (citations omitted) (emphasis added).

n104. *Id.* at 333 (citations omitted).

n105. *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (citing 47 U.S.C. 230(b)(5) (1998)).

n106. *Id.*

n107. 47 U.S.C. 230(a) (1998).

n108. 47 U.S.C. 230(b).

n109. 47 U.S.C. 230(c).

n110. *Zeran*, 129 F.3d at 330-31.

n111. 992 F. Supp. 44 (D.D.C. 1998).

n112. See *id.* at 47.

n113. *Id.* at 48 (quoting *Digital Equip. Corp. v. Altavista Tech., Inc.*, 960 F. Supp. 456, 462 (D. Mass. 1997)).

n114. *Id.* at 47.

n115. *Id.* at 48 n.7 (quoting Bruce W. Sanford & Michael J. Lorenger, *Teaching an Old Dog New Tricks: The First Amendment in an Online World*, 28 *Conn. L. Rev.* 1137, 1142 (1996)).

n116. *Id.* at 49.

n117. *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 n.1 (4th Cir. 1997).

n118. See *Zeran v. Diamond Broad. Inc.*, 203 F.3d 714, 717 (10th Cir. 2000).

n119. See *id.*