Washington Law Review

Volume 80 | Number 2

5-1-2005

Rebooting Cybertort Law

Michael L. Rustad

Thomas H. Koenig

REBOOTING CYBERTORT LAW

Michael L. Rustad & Thomas H. Koenig*

Abstract: Cyberspace provides an ideal legal environment for tortfeasors and online criminals because Internet Service Providers (ISPs) have no duty to mitigate harms caused by ongoing torts, crimes, and infringing acts. Courts have stretched Congress's express language in § 230 of the Communications Decency Act from the narrow purpose of immunizing ISPs as publishers to the expanded purpose of shielding them from all tort liability. This Article proposes imposing a limited duty of care on ISPs to remove or block ongoing tortious activities on their services when they have been given actual notice. This reform will harmonize American ISP liability law with the European Union's Electronic Commerce Directive, which imposes an affirmative duty on ISPs to take down objectionable materials. It also will unify U.S. law by creating procedures consistent with the takedown policy mandated by the Digital Millennium Copyright Act.

* Michael L. Rustad, Ph.D., J.D., LL.M., is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School in Boston, Massachusetts. Professor Thomas H. Koenig, Ph.D., M.A., chairs Northeastern University's Sociology Department and is on the Executive Committee of the Law, Policy & Society Doctoral Program.

It is a pleasant duty to write this Article to honor the memory of our teacher and friend, Thomas F. Lambert Jr. Tom Lambert was a major figure in American tort law who inspired jurists such as Roger Traynor, Allen Linden, and judges throughout the country. As tort law's most ardent defender, he gave lectures at bar associations and law schools in every state of the union. Tom's life and writings guided many of his students at the law schools of Boston University and Suffolk University into careers in consumer law and the trial bar. The Honorable Judge Edward Harrington of the United States District Court for the District of Massachusetts provided a useful critique of an earlier version of this Article. Professor Richard Delgado made useful substantive and stylistic suggestions. Diane D'Angelo assisted us expertly, as did research assistants Patricia Emrich and Peter Nechtem. We are grateful for their help. Sandra Paulsson, J.D., LL.M., who is a Trainee at the Policy Department for Economics and Science at the European Parliament in Brussels, sent us illuminating material. Al Frank, P.M.P., provided expert advice on Internet security. We also appreciate the helpful comments of Chryss J. Knowles on the manuscript.

INTRODUCTION

Cyberspace offers unscrupulous people an entirely new venue in which to conduct harmful activities without a significant chance of being identified, let alone punished. In the first half of 2004, the most common online frauds involved non-delivered merchandise, Nigerian money offers,[1] "phishing" for personal data,[2] and deceptive adult pornographic

1. Many variants of the Nigerian money swindle exist. One version involves an e-mail purporting to be from a Nigerian banker offering the recipient the opportunity to earn hundreds of thousands of dollars. Generally, the scamster poses as a representative of a dead multimillionaire. "He says he needs a foreign bank account through which to launder the money—and in return for sending him your bank details for this purpose, he will give you a share of the spoils." Will Sturgeon, *'Nigerian' Money Scam: What Happens When You Reply?*, The Spam Report, *at* http://www.silicon.com/research/specialreports/thespamreport/0,39025001,10002928,00.htm (Feb. 18, 2003).

2. The Internet has spawned new consumer injuries such as "phishing":

> In computing, phishing is the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by masquerading in an official-looking email, IM [instant message], etc. as someone trustworthy with a real need for such information. It is a form of social engineering attack. The term was coined in the mid

services.[3]

To illustrate the prevalence of Internet fraud, one of the Authors answered a Yahoo! advertisement that offered to sell a used 2001 Porsche Boxster for less than half its Kelley Blue Book value. The seller provided no address, telephone number, or other information verifying his identity. The fraudulent merchant attempted to bolster confidence by agreeing to meet in person so the Authors could inspect the automobile. Shortly before the scheduled meeting, the seller sent the following e-mail:

> sorry . . . but right now i'm not in the states. i urngent had to leave because my wife is seak . she have a malformation to teh heart and she needs a special operation in a specialised clinic in France. i must tell you that if you have real intentions about the car first you must make a deposit of 10% of the car price before teh shipping. sorry but I need buyers with real intentions because if i will not get the money for the operation in time my wife could die. my intentions are to sell the car to the first buyer who will make the deposit. if you are decided about buying the car please send me your full name and addres so I can arrange the shipping.[4]

The previous example is not an isolated occurrence. When one of the Authors sent e-mails expressing interest in two different models of Porsche automobiles on the Yahoo! website, the purported sellers responded using similar language:

> Thank you for your interest in my car. First of all, I want to tell you that the vehicle is in perfect condition. The milage is accurate. It has no scratches, no damages, no hidden defects. Kept it in a warm garage. It comes with all the documents needed for registration in US, it has a clear title issued in US and it can be anytime registred into your name any time without a problem so, I want you to stay cool about this. Also, the car will

---

1990s by crackers attempting to steal AOL accounts. An attacker would pose as an AOL staff member and send an instant message to a potential victim. The message would ask the victim to reveal his or her password, for instance to "verify your account" or to "confirm billing information." Once the victim gave over the password, the attacker could access the victim's account and use it for criminal purposes, such as spamming.

Wikipedia, The Free Encyclopedia, *Phishing*, *at* http://en.wikipedia.org/wiki/Phishing (last visited March 28, 2005).

3. National Fraud Information Center, *Internet Fraud Statistics: January to June 2004*, *at* http://www.fraud.org/janjune2004ifw.htm (last visited Mar. 22, 2005).

4. E-mail from Anonymous Seller to Michael L. Rustad (Aug. 20, 2004) (on file with authors).

> be delivered from Greece and I will take care of all shipping and insurance charges. I made a couple of phone calls and the best and fastest way I can ship the unit with DHL Air First door-to-door and you received it between 3-5 days. I hate to sell it, but after long discussions with my wife, we decided to invest the money that we will get from this in our future business. The price I hope to obtain for this beauty is $10000USD (this price of course includes shipping and insurance charges).[5]

The second "seller" responded:

> I will need first a deposit at Westen Union for $3000 so I can take care of the shipping, handleing and custom fees so when the car will get into US you wont have to pay a penny extra that the balance due delivery. You can pay that to DHL with a certifyed check and I will get the money from them. . . . As soon as the package arrives, you will test the item and if it does not matches 100% to your expectations, you will return it in max. 15 days since the arrival date. In this case I will send you the money back and after you received your money back, you will send me the car in the original crate and you don't have to pay the return shipping and insurance. If you agree with this price we can start the arrangements at this point. If you want to conclude this deal on the phone please tell me and I will call you. My best wishes and I'm waiting your response.[6]

As the old adage warns, "If it looks too good to be true, it is!" Consumers filed more than 24,000 complaints against online swindlers in the first six months of 2004.[7] These deceived consumers lost an average of $843 per transaction with cyberspace fraudsters.[8] During this same period, not a single online consumer received a monetary or equitable remedy from any Internet Service Provider (ISP)[9] in a

5. E-mail from Anonymous Seller to Michael L. Rustad (Aug. 27, 2004) (on file with authors).

6. E-mail from Anonymous Seller to Michael L. Rustad (Aug. 21, 2004) (on file with authors).

7. National Fraud Information Center, *supra* note 3.

In the fall of 2003, eBay removed the link from its Web site to the National Consumers League's fraud center. As a result, the number of auction complaints reported to NCL has dropped to 1/6 of the previous level. Based on statistics prior to eBay's action, NCL estimates that the fraud center would have received 18,660 auction complaints during the January 1–June 30, 2004 time period. The total number of Internet fraud complaints was projected at 24,505, with auctions representing 76%.

Id.

8. *Id.*

9. Professors Ronald J. Mann and Jane K. Winn define the term "ISP" to subsume "a variety of activities: from the wholly anonymous transmission of a backbone provider, to the wholly

cybertort lawsuit. A defrauded Internet consumer[10] has no recourse against a website or Internet portal that hosts a fraudulent seller, even if the intermediary had actual knowledge of ongoing cybercrimes. Consequently, if a victim of the auto sales scheme had notified Yahoo! of the pattern and practice of fraud on its online website, Yahoo! would have had no duty to take the seller offline or even to warn consumers to exercise caution when ordering goods from the seller.

Under current United States law, consumers are left without cybertort remedies against ISPs, even though ISPs are generally in the best position to mitigate damages from online fraudulent schemes, website defamation, and other information-based torts by taking down objectionable content. Congress expressly provided ISPs with protection from online defamation claims for publisher's liability when it enacted § 230 of the Communications Decency Act of 1996 (CDA).[11] Congress

---

transmissive service that a commercial ISP provides to a domain like utexas.edu, to the partially content-based activity that a provider like AOL, MSN, or Yahoo! provide to one of their subscribers." RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 177 (2d ed. 2005). For purposes of the Digital Millennium Copyright Act, an Internet "service provider," or ISP, is "a provider of online services or network access, or the operator of facilities therefore." 17 U.S.C. § 512(k)(1)(B) (2000).

In this Article, we define the term "ISP" broadly. We use the term ISP to refer to an "interactive computer service" as defined by § 230 of the Communications Decency Act of 1996 (CDA): 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 and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2) (2000). The "interactive computer service" broadly encompasses large-scale and small-scale service providers, search engines, websites, and many other online intermediaries. Courts may define ISPs more narrowly as entities that "provide[] . . . subscribers with access to the Internet. Such service providers include, for example, America Online, commonly referred to as 'AOL,' and Earthlink, as well as numerous other providers." Batzel v. Smith, 333 F.3d 1018, 1028 n.12 (9th Cir. 2003).

10. For purposes of our study, the Authors defined "consumer" as an individual buying goods for "personal, family, or household purposes." For example, the term "consumer debt" in the federal bankruptcy statute is defined to include "debt incurred by an individual primarily for a personal, family, or household purpose." 11 U.S.C. §101(8) (2000). "The definition [of consumer debt used in the bankruptcy act] is adapted from the definition used in various consumer protection laws." H.R REP. NO. 95-595, at 309 (1977), *reprinted in* 1978 U.S.C.C.A.N. 5963, 6266; S. REP. NO. 95-989, at 22 (1978), *reprinted in* 1978 U.S.C.C.A.N. 5787, 5808. For example, the Authors' definition of consumer is found in the federal Truth in Lending Act (TILA). 15 U.S.C. § 2301(1) (2005) (defining term "consumer product" to include "any tangible personal property which is distributed in commerce and which is normally used for personal, family, or household purposes"). TILA's scope is limited to "consumer" credit transactions, which are defined as transactions in which "the money, property, or services which are the subject of the transaction are primarily for personal, family, or household purposes." 15 U.S.C. § 1602(h) (2000); 12 C.F.R. § 226.2(p) (2004). Similarly, a consumer transaction in cyberspace includes commercial transactions in which an individual purchases goods or services online for personal, family, or household purposes.

11. Communications Decency Act of 1996, Pub. L. No. 104-104, title V, 110 Stat. 133, 133–143

did not address the larger question of whether ISPs were also immunized from online defamation liability when they act as mere distributors of defamatory statements. U.S. courts have stretched the CDA to abolish ISPs' common-law liability as distributors, even when ISPs know or have reason to know of underlying defamatory content.[12] As a result, online service providers enjoy total immunity from liability as both distributors[13] and as publishers.[14]

(codified as amended at scattered sections of 47 U.S.C.). "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." 47 U.S.C. § 230(c)(1) (2000). The primary goal of the CDA was to control the exposure of minors to indecent material. *See* Communications Decency Act of 1996, Pub. L. No. 104-104, title V, 110 Stat. 133, 133–143 (codified as amended at scattered sections of 47 U.S.C.); H.R. REP. NO. 104-458, at 81–91 (1996) (noting statutory purpose of protecting children from being exposed to pornographic materials online); S. REP. NO. 104-230, at 187–93 (1996) (same); S. REP. NO. 104-23, at 9 (1995) (same). Section 230 authorizes providers and users of interactive computer services to remove or restrict access to inappropriate materials without being classified as publishers. 47 U.S.C. § 230(c)(2).

12. *See infra* Part II.

13. Distributors include conduits such as "telegraph and telephone companies, libraries and news vendors." DAN B. DOBBS, THE LAW OF TORTS § 402, at 1123 (2000). Distributors do not have liability for content created by others unless "the distributor knows or should know of the defamatory content in materials he distributes." *Id.* A bookstore owner, for example, would not be liable for defamatory statements made in books the store sold absent actual knowledge. "ISPs and other distributors of information (e.g., bookstores) only assume liability when they acquire knowledge of the material they are handling." Brian C. Lewis, Note, *Prevention of Computer Crime Amidst International Anarchy*, 41 AM. CRIM. L. REV. 1353, 1368 (2004) (citing 47 U.S.C. § 230 (2000)). The common law rule makes a distributor liable where it has knowledge of the facts and circumstances that are producing clearly libelous activity, but takes no action to remove the material. *See, e.g.*, Lerman v. Chuckleberry Publ'g, Inc., 521 F. Supp. 228, 235 (S.D.N.Y. 1981) ("[D]istributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation."), *reversed on other grounds*, Lerman v. Flynt Distrib. Co., Inc., 745 F.2d 123 (2d Cir. 1984). The Restatement Second of Torts explains:

> [A] news dealer is not liable for defamatory statements appearing in the newspapers or magazines that he sells if he neither knows nor has reason to know of the defamatory article. The dealer is under no duty to examine the various publications that he offers for sale to ascertain whether they contain any defamatory items. Unless there are special circumstances that should warn the dealer that a particular publication is defamatory, he is under no duty to ascertain its innocent or defamatory character. On the other hand, when a dealer offers for sale a particular paper or magazine that notoriously persists in printing scandalous items, the vendor may do so at the risk that any particular issue may contain defamatory language.

RESTATEMENT (SECOND) OF TORTS § 581 cmt. d (1977).

14. Section 230 federal immunity for service providers is far broader than that offered in European countries. The United Kingdom, for example,

> adapts the traditional innocent disseminator defence to the on-line environment. It does not provide the *carte blanche* protection from liability that s. 230 of the American [CDA] does. An ISP, which by virtue of s. 1(3) is not an author, editor, or publisher; that takes reasonable care, having regard to the factors listed in s. 1(5); and does not know or have reason to believe that what he did caused or contributed to the publication of a defamatory statement, will be protected from liability for defamation.

The judiciary's inflated interpretation of § 230 has created a legal environment that is ideal for injury and difficult for redress. ISPs have no obligation to remove tortious materials, to prevent the reposting of objectionable materials, or to help victims track down the primary wrongdoers. Consequently, cyberspace injuries resulting from online stalking, defamatory messages posted to Internet newsgroups, dark-side hackings, e-mail spam, online espionage, or the unleashing of destructive computer viruses generally go unpunished by the civil law. Consumers have the right to pursue primary wrongdoers through tort litigation, but this is rarely a realistic option because the typical cybercriminal finds it easy to default by disappearing to an unknown and unknowable foreign venue.[15]

In *Does 1 Through 30 Inclusive v. Franco Productions, Inc.*,[16] for example, a jury awarded more than $500 million in damages to a group of college athletes who, while showering and in various stages of undress, were secretly videotaped by pornographers who sold the tapes on a website.[17] The plaintiffs have no significant hope of collecting this award from the sellers of the videotapes because the defendants did not appear in court and defaulted.[18] The plaintiffs' appeal, therefore, was only against the ISPs that had profited from the fees they received for hosting the websites that sold the obscene materials.[19] The United States Court of Appeals for the Seventh Circuit dismissed all claims against these solvent web hosts, ruling that § 230 immunized these ISPs from all liability.[20] The victimized athletes were thus left without any meaningful legal recourse. Similar injustices can be redressed only by reducing the judicially expanded broad immunity for online torts enjoyed by ISPs.

As in the industrial age, the common law of torts must now

Michael Deturbide, *Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses*, J. INFO. L. & TECH., pt. 6.1 (Issue Three) (2000), *at* http://elj.warwick.ac.uk/jilt/00-3/deturbide.html.

15. *See, e.g.*, Doe v. GTE Corp., 347 F.3d 655, 656 (7th Cir. 2003) (describing how primary wrongdoers defaulted or could not be located or served with process in Internet tort action).

16. 2000 U.S. Dist. LEXIS 8645 (N.D. Ill. June 22, 2000), *aff'd sub nom.* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

17. *Id.* at *14–16 (failing in attempt to breach service provider immunity in order to include invasion of privacy action against web hosts selling objectionable online content).

18. *GTE*, 347 F.3d at 656.

19. Judge Easterbrook noted that there was little prospect of collecting from the primary wrongdoer. *Id.* at 657.

20. *Id.* at 659.

accommodate itself "to the changing thought and action of the times."[21] Internet tort remedies need to evolve beyond their current role of protecting the interests of powerful Internet stakeholders so that the civil law can respond to the new risks and dangers lurking on the World Wide Web. The ideal Internet tort regime for the twenty-first century would be highly adaptable and supremely flexible in order to punish and deter those who commit online defamation, fraud, or other information torts. America's tort regime has yet to achieve its potential as a defender of the victims of cyberwrongs because absolute immunity permits ISPs to behave irresponsibly without suffering any consequences.

This Article reconceptualizes the tort liability of online intermediaries such as ISPs, websites, and search engines to help consumers redress online injuries.[22] Part I draws upon a database of cyberspace cases to show that, while cybertorts are developing to protect corporate interests, the online consumer has little recourse in tort law.[23] Thus, victims of fraudulent online auctions and online sales, Nigerian money offers, fake check scams, online privacy invasion, and a variety of other cyberspace injuries have rights without effective remedies.

Part II traces the path of Internet law, focusing on the cybertort liability of online intermediaries. Congress substantially altered the cybertort landscape by enacting § 230 of the CDA. Congress intended this section to shield ISPs from traditional publisher liability for content supplied by third parties.[24] Courts, however, have expanded § 230 far

21. 1 FOWLER V. HARPER ET AL., THE LAW OF TORTS xxvi (3d ed. 1996) (describing how common law of torts, property, and contract has historically been adaptable); *see also* Ezra Dodd Church, Note, *Technological Conservatism: How Information Technology Prevents the Law from Changing*, 83 TEX. L. REV. 561, 581–86 (2004) (explaining how software code and nature of information technologies creates legal lag).

22. Search engines are "on-line tools used for finding Web sites . . . . There are two types of search engines, namely, 'automated' search engines and search engines that rely upon people to review and catalogue Web sites." Pablo Asbo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 111, 116 (2002).

23. We have updated our empirical study of litigation to include all Internet-related litigation between January 1, 1992, and July 1, 2004, in which a prevailing plaintiff received either monetary damages or equitable relief. For a fuller description of the methodology used to create the earlier database, see generally Michael L. Rustad, *Punitive Damages in Cyberspace: Where in the World Is the Consumer?*, 7 CHAPMAN L. REV. 39 (2004); Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77 (2003).

24. Congress enacted § 230 to expressly overrule courts that would hold ISPs liable as publishers for materials posted by third parties.

> [Congress] worried that such a rule would deter a provider of an interactive computer service from removing objectionable material from its services that are frequented by minors because removing the material would subject the service provider to publisher liability. In response,

beyond Congress's original intent by immunizing ISPs and websites from distributor liability and virtually every other tort action.[25]

Part III examines the injustice experienced by consumers who fail to find any legal redress for injuries, losses, or damages that result from the negligent or intentional acts of cybertortfeasors and cybercriminals. 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. The most critical issue is whether ISPs owe a duty to take down objectionable content or to help their customers track down third-party criminals. While ISPs are not insurers of their customers' safety, they should have a duty to remove content that is known to be tortious or criminal.

Part IV proposes that Congress scale back § 230's absolute immunity for ISPs by reformulating online intermediary law to harmonize elements from the common law of distributor liability, the Digital Millennium Copyright Act's (DMCA) notice-and-takedown procedure,[26] and the European Union's E-Commerce Directive.[27] Under our proposed cybertort takedown policy, an ISP would not be liable for third-party defamation until it received actual notice of objectionable content and failed to take prompt remedial action to avoid further losses.[28] This

---

Congress enacted 47 U.S.C. § 230 as part of the CDA.

Ryan W. King, *Online Defamation: Bringing the Communications Decency Act of 1996 in Line with Sound Public Policy*, 2003 DUKE L. & TECH. REV. 0024, ¶ 4, *at* http://www.law.duke.edu/journals/dltr/articles/PDF/2003DLTR0024.pdf.

25. *See infra* Part II.B.

26. Digital Millennium Copyright Act, Pub. L. 105-304, § 202, 112 Stat. 2860, 2879–2881 (1998) (codified as amended at 17 U.S.C. § 512(c) (2000)). The notice-and-takedown procedure is described at 17 U.S.C. § 512(c).

27. *See* Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce'), 2000 O.J. (L 178) [hereinafter E-Commerce Directive] (discussing certain legal aspects of information society services, in particular electronic commerce, in the internal market of the European Community), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf (last visited Apr. 24, 2005). The E-Commerce Directive harmonizes rules for all European countries for commercial communications, electronic contracts, and limitations of liability of intermediary service providers. The European Union (EU) is an international organization of European countries that forms common institutions. Europa, *The European Union at a Glance*, *at* http://europa.eu.int/abc/index_en.htm (last visited Apr. 24, 2005). The EU's five major institutions are the European Parliament, Council of The European Union, European Commission, Court of Justice, and Court of Auditors. *Id.* EU decisions and procedures are based on treaties between the member states. *Id.* Directives require all EU member states to enact legislation to implement policies by a given date. *Id.*

28. "The intentional torts of fraud, deceit, or misrepresentation are information torts because the plaintiff has suffered loss in relying upon false or misleading statements made by defendants."

reform would arm content providers that are victimized by frivolous or bad faith takedown demands with the right to a federal court hearing, as well as rights to legal or equitable remedies. This safeguard against inappropriate takedown demands will punish and deter the use of strategic takedown demands that have the potential to chill free speech on the Internet.

Imposing this limited liability on ISPs is a crucial first step toward permitting tort law to evolve to punish and deter online fraud, online sexual harassment, invasion of privacy, and numerous other Internet injuries.[29] Tort law has historically progressed through dramatic legal cases or developments that abolished unjust barriers to obtaining restitution.[30] Breaching the citadel of ISP immunity will catalyze further legal reforms that will protect consumers on the World Wide Web. Instituting website liability for illegal postings has the potential to jumpstart the field of cybertorts so that it can develop into an effective social control mechanism for cyberspace.

I. AN OVERVIEW OF CYBERTORTS: A NEW AUDIT

> *Existing rules and principles can give us our present location, our bearings, our latitude and longitude. The inn that shelters for the night is not the journey's end. The law, like the traveler, must be ready for the morrow. It must have a principle of growth.*[31]

This Part presents data from a statistical study of cyberlaw remedies to show that new torts are evolving to protect the rights of ISPs,

---

Rustad & Koenig, *supra* note 23, at 94. Online defamation is the obvious example of an information tort because by definition it includes widely disseminated derogatory statements about individuals or entities. Many other traditional tort categories, such as assault, battery, or false imprisonment, are not yet problematic because the Web does not allow the necessary physical presence.

29. The topic of ISPs' direct tort liability is beyond the scope of this Article. Online intermediaries will have liability for their own direct torts, such as personal property torts, the invasion of privacy, negligently enabling the spread of viruses, or failing to prevent cybercrimes. The further expansion of ISP tort liability, the recognition of new duties of care, and the extension of traditional tort theories to new cyberspace injuries are necessary developments for the long-term welfare of consumers and other users.

30. Judge Cardozo's ground-breaking opinion in *MacPherson v. Buick Motor Co.*, 111 N.E. 1050 (N.Y. 1916), opened the door to development of products liability. The tort of invasion of privacy had its genesis in a law review article by Samuel Warren and Louis Brandeis. *See generally* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

31. BENJAMIN N. CARDOZO, THE GROWTH OF THE LAW 19–20 (2d ed. 1973).

websites, search engines, and other Internet corporate entities, while these same stakeholders are immunized from tort actions brought by consumers and other computer users.[32] Cybertort litigation reverses the pattern of traditional brick-and-mortar torts in which consumers vindicate their rights against corporate wrongdoers. Repeat players such as America Online, Inc. (AOL), Ford Motor Co., Mattel, Inc., and Hollywood media providers dominate the cyberlegal landscape as prevailing plaintiffs, but not as defendants.

Corporate stakeholders use their lobbying influence to expand their online rights and to avoid liability. In the past decade, Congress has enacted several statutes that have increased the power of the "haves" in cyberspace.[33] The DMCA, for example, provides Hollywood with new weapons to battle the downloading of copyrighted music and images.[34] The owners of famous trademarks have gained protections against dilution that are not available to small or medium businesses that have less well-known trade names.[35] Similarly, Congress enacted the

32. The research methodology, including sample selection, for this database is explained in Rustad & Koenig, *supra* note 23. The statistical database was updated from the earlier study, but the methodology for collecting and examining the data is the same. As in the earlier study, coding decisions were often difficult in determining what was a cybertort action. Many Internet-related cases, for example, included several causes of action. Spam-related cases invariably pleaded state and federal computer crime statutes in addition to the tort of trespass to chattels. Many intellectual property cases involved both the federal Lanham Act and a pendent tort cause of action. All cases were classified according to the central thrust or gravamen of the action. The analysis in Chart Three presents cases where the "predominant" cause of action was in tort or another substantive field.

33. *See generally* Jordana Boag, *The Battle of Piracy Versus Privacy: How the Recording Industry Association of America (RIAA) Is Using the Digital Millennium Copyright Act (DMCA) as Its Weapon Against Internet Users' Privacy Rights*, 41 CAL. W. L. REV. 241 (2004) (arguing that large copyright stakeholders are subordinating privacy rights of consumers by deploying new statutory remedies protecting intellectual property).

34. The DMCA armed the entertainment industry with new remedies against circumvention devices designed to decrypt the contents of DVDs. *See* 17 U.S.C. §§ 1201, 1202(b) (2000). The peer-to-peer file sharing movement on the Internet pits the movie, record, and film industries against Internet users. In *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1005, 1027 (9th Cir. 2001), the United States Court of Appeals for the Ninth Circuit upheld a federal court order enjoining Napster from facilitating the wholesale copying of music on its service. *See also* Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 213 (S.D.N.Y. 2000) (enjoining websites from posting the software which circumvents anti-copying software controls on DVDs).

35. The Federal Trademark Dilution Act (FTDA) provides new remedies for the dilution of famous trademarks. The court determines whether a trademark is famous by balancing eight statutory factors. Federal Trademark Dilution Act of 1995, Pub. L. 104-98, sec. 3, § 43, 109 Stat. 985, 985–986 (codified as amended at 15 U.S.C. § 1125(c)(1) (2000)). The eight FTDA factors include the duration and extent of use of the mark, the nature of the advertising, and the acquired distinctiveness of the mark. 15 U.S.C. § 1125(c)(1). These factors favor the marks of the largest and most powerful companies.

Anti-Cybersquatting Consumer Protection Act of 1999 (ACPA) to deter the unauthorized registration or use of trademarks as Internet domain names.[36]

In contrast, consumers and small businesses have no practical tort remedies against ISPs, websites, online information content providers,[37] or other cyberspace intermediaries. Entire categories of victims of Internet injuries, including defrauded consumers, victims of workplace snooping, and those whose personal or financial privacy has been invaded, lack any legal recourse against ISPs for online injuries. This legal regime is inefficient because the service provider, not the consumer, is generally in a superior position to determine whether an online scam artist falsified a transmission path, used open proxies to disguise the origin of e-mail messages, or used false contact information to carry out a fraudulent scheme.[38] If the ISP community owed a greater duty to its subscribers, it would have incentives to develop technological solutions to the problem of consumer fraud.[39]

Cyberspace law is flourishing when it comes to electronic evidence,[40]

---

36. *See* 15 U.S.C. § 1125(d)(1)(B) (stating that trademark holders should be protected from misuse of domain names intending to "divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion").

37. The CDA defines an "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3) (2000).

38. Service providers are almost always in the best position to develop authentication technologies to restrain spammers who use false identities for the sole purpose of sending spam to millions of consumers. AOL's Vice Chairman estimated

> that more than 80% of the current spam problem comes from other ISPs and hosting companies that are infested with viruses. These software viruses, or "trojans" as we refer to them, typically make their way onto machines via vulnerabilities in end-user software and the absence of firewalls or anti-virus software. These viruses/trojans infect users' computers without their knowledge and allow spammers to use the infected machines to initiate or relay spam.

Growing Problem of Spam: Hearing on CAN-SPAM Act Before the Sen. Comm. on Commerce, Sci. and Transp., 108th Cong. (2004) (statement of Ted Leonsis, Vice Chairman, America Online, Inc.), *available at* http://commerce.senate.gov/hearings/testimony.cfm?id=1199&wit_id=3436 (last visited Apr. 25, 2005).

39. In a Senate committee hearing, the Vice Chairman of AOL proposed further investigation of several spam-fighting methods:

> (1) for all ISPs to confirm that their members who are sending e-mail have accounts and are allowed to send mail; and (2) for abuses indicated by ISP members to be handled as quickly as they arise. We are continuing to work with our ISP colleagues to develop additional solutions to the spam problem, both from a technology and enforcement perspective.

Id.

40. "Today it is black letter law that computerized data is discoverable if relevant." Anti-

domestic cyberpiracy,[41] online gambling,[42] Internet advertising,[43] cybersquatting,[44] spamming,[45] linking,[46] online music piracy,[47] Internet

---

Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995). The Federal Rules of Civil Procedure were revised to include a new rule requiring litigants to turn over electronic data. *See* FED. R. CIV. P. 26(a)(1) advisory committee's note (1993 Amendments). Electronic smoking guns are the star witnesses in a growing number of cases. *See, e.g.*, Knox v. Indiana, 93 F.3d 1327, 1330 (7th Cir. 1996) (citing e-mail messages from one employee to another asking plaintiff whether she wished "horizontal good time"); Comiskey v. Automotive Indus. Action Group, 40 F. Supp. 2d 877, 888 (E.D. Mich. 1999) (finding sexually charged e-mails served as part of harassment claim); Harley v. McCoach, 928 F. Supp. 533, 540 (E.D. Pa. 1996) (noting that e-mails documented racial discrimination).

41. In *Panavision International v. Toeppen*, 938 F. Supp. 616 (C.D. Cal. 1996), a domain name cyberpirate was found liable in a lawsuit in California because his attempt to sell a domain name containing a corporation's famous trademark was deemed sufficient for jurisdiction. *Id.* at 622. The defendant appealed this decision, and the Ninth Circuit affirmed personal jurisdiction in the trademark case filed by owners of the marks PANAVISION and Panaflex. Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1322 (9th Cir. 1998). The defendant cybersquatter had registered the domain names panavision.com and panaflex.com, and posted pictures of Pana, Illinois, on one website and the word "hello" on the other. *Id.* at 1319. He then attempted to sell the domain names to Panavision. *Id.* The court premised jurisdiction on the defendant's intention of doing business in California and his tortious attempt to extort money from a California trademark owner. *Id.* at 1321–22. The court upheld jurisdiction, employing the "effects test." *Id.* at 1321.

42. In *Rio Properties, Inc. v. Rio International Interlink*, the plaintiff casino operator sued a foreign Internet gambling business, claiming that the defendant infringed the plaintiff's trademark. Rio Props., Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1012 (9th Cir. 2002). The plaintiff served the gambling business by regular mail to its attorney and its international courier, and by e-mail to its Internet address. *Id.* at 1013. The gambling business contended that service was insufficient and that personal jurisdiction was lacking. *Id.* at 1014. The court held that the alternative service was proper because the defendant actively evaded the conventional means of service attempted by the plaintiff. *Id.* at 1017. E-mail service was an appropriate alternative as the method of communication preferred by the defendant. *Id.* The defendant's advertisements in the forum state and the injury to the plaintiff in the forum state were sufficient to provide personal jurisdiction over the gambling business. *Id.* at 1021.

43. Private litigants may use state and federal deceptive trade practices acts to enjoin fraudulent Internet advertising. For instance, a hotel chain sued Gator.com for its pop-up banner advertisements under, inter alia, a state's deceptive trade practices act. *E-Commerce Legislative Update*, 19 E-COMMERCE L. & STRATEGY 10 (2002) (citing Six Continents Hotels, Inc. v. Gator Corp., No. 1 02-CV-3065 (N.D. Ga. Nov. 12, 2002)). The hotel also claimed that Gator's pop-up advertisements infringed its registered trademarks and copyrights. *Id.*

44. "Cybersquatting is the act of registering a popular Internet address—usually a company name—with the intent of selling it to its rightful owner." Webopedia, *Cybersquatting*, *at* http://www.webopedia.com/TERM/C/cybersquatting.html (last visited Mar. 28, 2005); *see, e.g.*, Catalina Mktg. Int'l, Inc. v. CoolSavings.com, Inc., 289 F.3d 801, 810 (Fed. Cir. 2002) (reversing patent victory in favor of dot.com company); Amazon.com, Inc. v. Barnesandnoble.com, Inc., 239 F.3d 1343, 1347 (Fed. Cir. 2001) (vacating preliminary injunction awarded in favor of Amazon.com in patent dispute over one-stop Internet shopping business method); Cable News Network L.P., L.L.L.P. v. cnnews.com, 162 F. Supp. 2d 484, 494 (E.D. Va. 2001) (holding that plaintiff properly perfected service under ACPA's in rem service procedure in domain name litigation); E. & J. Gallo Winery v. Spider Webs Ltd., 129 F. Supp. 2d 1033, 1037 (S.D. Tex. 2001) (enjoining domain name

taxation,[48] and the problem of obtaining personal jurisdiction.[49] In less than a decade, U.S. courts have forged new rules for e-commerce patents[50] and the law of e-commerce.[51] In our book, *In Defense of Tort*

---

registrant from violating famous winemaker's trademarks); Mattel, Inc. v. Adventure Apparel, No. 00 Civ. 4085 (RWS), 2001 U.S. Dist LEXIS 13885, at *13 (S.D.N.Y. Sept. 6, 2001) (finding cybersquatting in case where defendant registered domain names "barbiesbeachwear.com" and "barbiesclothing.com" and "parked" them at Adventure Apparel website); Mattel, Inc. v. Internet Dimensions, Inc., No. 99 Civ. 10066 (HB), 2000 U.S. Dist. LEXIS 9747, at *18 (S.D.N.Y. July 13, 2000) (finding specific jurisdiction in domain name action involving cybersquatting claim in which adult entertainment website was enjoined from using famous Barbie trademark owned by Mattel).

45. Spam e-mail is not merely a minor irritation, but a drain on American productivity. "Rebutting a recent finding that spam is not a drain on worker productivity, [a] San Francisco-based market research company . . . has estimated that unwanted commercial e-mail cost U.S. corporations $8.9 billion in 2002." Brian Morrissey, *Spam Costs Corporate America $9 Billion in 2002*, *at* http://www.clickz.com/stats/sectors/demographics/article.php/1565721 (last visited Mar. 24, 2005). In *Cyber Promotions, Inc. v. America Online, Inc.*, 948 F. Supp. 436 (E.D. Pa. 1996), the court ruled that an e-mail spammer did not have a First Amendment right to send massive amounts of unsolicited, commercial e-mail to Internet subscribers. *Id.* at 445.

46. Ford Motor Co. v. 2600 Enters., 177 F. Supp. 2d 661, 662, 666 (E.D. Mich. 2001) (denying injunctive relief to Ford Motor Co., which sought to enjoin defendants from maintaining domain name, "FuckGeneralMotors.com," that takes user directly to Ford Motor Co.'s official website at "ford.com"); Bernstein v. JC Penney, Inc., 50 U.S.P.Q.2d (BNA) 1063, 1063–64 (C.D. Cal. 1998) (dismissing claim that link to infringing materials constituted copyright infringement).

47. "It is estimated that 1 million illegal music files are posted on the Internet—yet few countries outside the USA have adequate legislation to fight Internet piracy." Profile Publ'g & Mgmt. Corp. APS v. Musicmaker.com, 242 F. Supp. 2d 363, 364 (S.D.N.Y. 2003) (quoting one party's exhibit).

48. *See* Meghan Holohan, *California May Pass Internet Sales Tax*, COMPUTERWORLD, *at* http://www.computerworld.com/industrytopics/retail/story/0,10801,49311,00.html (Aug. 31, 2000) (reporting that California State Senate passed bill that, "if approved by the state Assembly and signed by the governor, will require all California-based companies to add sales tax to online purchases"). *But see* Jon Weisman, *California Governor Vetoes Net Tax Bill*, E-COMMERCE TIMES, *at* http://www.ecommercetimes.com/story/4384.html (Sept 26, 2000) (noting that Governor Gray Davis vetoed proposed law that would have required California businesses to charge sales tax for in-state online transactions). *See also* Jeffrey M. Vesely & Richard E. Nielsen, *Federal and California Internet Tax Freedom Acts—What Do They Mean?*, ST. & LOC. TAX BULL. (Pillsbury Winthrop Shaw Pittman LLP, San Francisco, Cal.), July 2000, at 6 (explaining three-year moratorium placed on Internet taxes by Internet Tax Freedom Act, Pub. L. 105-277, Div. C., title xi, 112 Stat. 2681, 2681–2719 (1998)), *available at* http://www.pmstax.com/ftp/state/bull0007.pdf (last visited Apr. 24, 2005).

49. Many U.S. courts have found that a plaintiff in an Internet-related case satisfies due process by showing that: (1) the defendant purposefully availed itself of the privilege of conducting activities in the forum state by invoking the benefits and protections of the forum state's laws; (2) the plaintiff's claim arises out of the defendant's forum-related activities; and (3) the exercise of jurisdiction over the out-of-state defendant is reasonable. MICHAEL L. RUSTAD & CYRUS DAFTARY, E-BUSINESS LEGAL HANDBOOK § 7.03 (2003).

50. No single development has spurred the growth of Internet-related patents more than *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, 149 F.3d 1368, 1373 (Fed. Cir. 1998) (validating business method patent based on mathematical algorithms).

Law, we made the rosy prediction that new torts were on the horizon to protect consumers in cyberspace.[52] 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.

A. Repeat Players Dominate the Internet Legal Landscape

Repeat players shape the Internet litigation environment because they have extensive financial and legal resources as well as invaluable prior experience in vindicating their intellectual property, contract, and tort rights. Marc Galanter's classic essay, "Why the 'Haves' Come Out Ahead," explained the great advantages that powerful corporate entities have in maneuvering through the obstacle course of administrative agencies as well as in the courtroom.[53] "Repeat players" generally prevail over "one-shotters" in cases that settle or go to trial because of their greater wealth and access to the specialized knowledge that is provided by national law firms.[54] Consumers are the classic example of "one-shotters" who lack the resources to vindicate their rights in cyberspace. They typically cannot afford to retain a lawyer, let alone the top legal talent needed to untangle complex issues such as serving process to defendants in other countries, establishing personal jurisdiction in cyberspace, or locating the assets of cyber-wrongdoers that have been hidden in secret cross-border locations.[55]

---

51. The growth of the Internet involves updating and adapting common law principles to cyberspace:

> [Richard] Nixon's observation that courts were developing new rights and remedies to adjust to an emerging technology applies equally well to the contemporary age of the Internet. Just as in Nixon's day, the rise of a new technology requires courts to stretch traditional tort doctrines as well as to create updated torts to keep pace with new civil wrongs.

Rustad & Koenig, *supra* note 23, at 77. *See generally* Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under the Federal E-SIGN Legislation and the UETA*, 56 BUS. LAW. 293 (2000) (discussing state electronic commerce legislation in a number of jurisdictions and comparing state to federal developments).

52. THOMAS H. KOENIG & MICHAEL L. RUSTAD, IN DEFENSE OF TORT LAW 235–36 (2001).

53. *See generally* Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 L. & SOC'Y REV. 95 (1974).

54. *Id.* at 98–101 (arguing that certain well-heeled corporate entities, "repeat players," have huge advantages over "one-shotters" in seeking legal remedies because of mismatch in resources); Samuel Gross & Kent D. Syverud, *Don't Try: Civil Jury Verdicts in a System Geared to Settlement*, 44 UCLA L. REV. 1, 52–53 (1996) (citing examples of how "repeat players" enjoy strategic advantages over "one-shotters" in settlement).

55. According to one commentator:

Without the prospect of locating a solvent primary wrongdoer who can be served with legal process, the only available defendant is the ISP, which is immunized from tort liability. Consumers and other computer users are generally left without any meaningful redress for their injuries, even if the facts and legal arguments are overwhelmingly in their favor. When there is little or no probability of detection or prosecution, predatory torts such as online fraud will skyrocket. "Cybertorts are now a fact of life for computer users. A recent report by Riptech, Inc. projects a sixty-four percent annual increase in Internet attacks against private and public organizations worldwide." [56] The cyberlaw litigation landscape reflects the hegemonic position of repeat players over one-shot consumers. When a consumer experiences financial loss, identity theft, or the malicious meltdown of their personal computer, the online cybercriminal almost always defaults or is not locatable. The primary wrongdoer is generally beyond the reach of jurisdiction, particularly because the ISP has no duty to aid in locating the origin of the illegal posting. Many consumer frauds, for example, originate in the new Russian Republics, which have become "a popular venue for innovative cyberscams involving credit card numbers stolen from websites." [57] While repeat players enjoy a favorable legal environment, consumers have no recourse against web hosts, websites, or service providers that benefit from selling advertising or providing other services for

---

The Internet offers low-cost communication, the capacity to reach a global audience, and a presumptive veneer of credibility stemming from the anonymity of cyberspace. Thus, Internet users may find it hard to distinguish genuine sources of information from fraudulent sources, creating a fertile environment for all kinds of Internet fraud.

Miriam R. Albert, *E-Buyer Beware: Why Online Auction Fraud Should Be Regulated*, 39 AM. BUS. L.J. 575, 578–79 (2002); *see* George P. Long, III, Comment, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1178–79 (1994). Even when consumers are able to unveil anonymous respondents, they face substantial procedural barriers in seeking redress against online defendants. Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1269–70 (N.D. Cal. 2001) (dismissing Wiretap Act claims against Amazon.com because online company simply received communication and did not "intercept" communication as required by Wiretap Act; also dismissing Electronic Communications Privacy Act claims because Amazon.com was online retailer rather than provider of electronic communication services or remote computing services as required under federal statute); Lieschke v. RealNetworks, Inc., Nos. 99 C 9274, 99 C 7380, 2000 U.S. Dist. LEXIS 1683, at *2 (N.D. Ill. Feb. 10, 2000) (enforcing RealNetworks' arbitration clause dismissing consumer's federal court decision).

56. Gordon A. Coffee & Charles B. Klein, *Combating Cyber-Torts: Protections and Pitfalls of the Virginia Computer Crimes Act*, 2 CYBERCRIME L. REP. 3, 3 (2002), *available at* http://www.winston.com/pdfs/CCLR110402.pdf.

57. Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 74 (2001).

cybercriminals. Consumers are left defenseless in cyberspace because immunized service providers are the only identifiable deep pocket. ISPs currently have no duty to police the Internet or to develop technologies to track down off-shore posters of objectionable materials.

Charts One, Two, and Three confirm that cybertort laws, particularly those that protect individuals from corporate misdeeds, illegal postings, and cybercriminals, have yet to develop. Our statistical analysis of the Internet legal landscape includes all U.S. dispositions where plaintiffs prevailed by receiving either an equitable or monetary damages award between January 1992 and July 2004.[58] We find that the cybertort landscape is a reverse image of the tort cases found in traditional civil litigation. Corporations frequently file cyberlaw cases in order to "push the envelope" on federal intellectual property statutes protecting their intangible assets.

Internet litigation is the only substantive branch of tort law where federal court filings are more common than state court litigation. During the seminal era of cyberspace litigation between 1992 and 2004, federal courts decided seventy-five percent of the cases.[59] This reflects the high proportion of intellectual property cases as compared to common law disputes, which are generally litigated in state court.[60] Repeat players such as ISPs have no qualms about protecting their rights through Internet lawsuits over intellectual property, tort, and contract rights, all of which are primarily resolved in federal courts. Consumers, in contrast, lack useful remedies against the unidentified perpetrators of Internet crimes and therefore do not file the common law tort claims that classically appear on state court dockets. The best tort reform would be to impose a limited duty on providers, which would motivate ISPs and other Internet "repeat players" to develop better methods of protecting consumers from third party crimes or torts.

---

58. These new empirical findings are consistent with findings from an earlier study of cyberlitigation for the period 1992–2002. Rustad & Koenig, *supra* note 23, at 86 (reporting 114 Internet-related cases in which there was at least one tort cause of action).

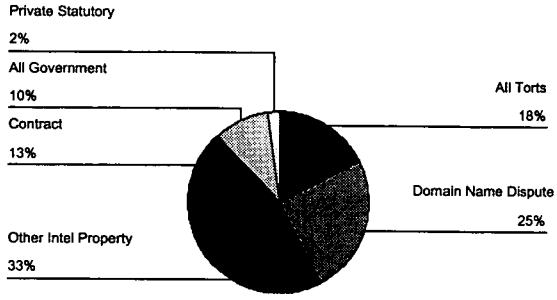
59. *See* Chart One, *infra* p. 352. Sixty-four percent of the business torts were decided in federal courts because the great majority of these cyberspace disputes were actions to protect trade secrets or other intellectual property rights on the Internet. Twenty-three of the thirty-six online defamation cases (64%) were decided in state courts. Of the nine online plaintiff's victories in privacy cases, six were litigated in state courts.

60. STEVEN K. SMITH ET AL., U.S. DEP'T OF JUSTICE, NCJ-153177, CIVIL JUSTICE SURVEY OF STATE COURTS, 1992: TORT CASES IN LARGE COUNTIES 2 (April 1995) (documenting state court dockets in largest U.S. cities for 1992), *available at* http://www.lectlaw.com/files/lit15.htm (last visited Apr. 24, 2005).

B. *Cyberlaw Generally Protects Corporate Repeat Players*

Chart One

Cyberspace Plaintiff Victories by Substantive Area



(Jan. 1992-July 2004) N=562

Chart One classifies prevailing plaintiffs by their principal cause of action in all successful Internet cases decided between January 1, 1992, and July 1, 2004.[61] As Chart One illustrates, intellectual property infringement claims account for fifty-eight percent of the decided cases.[62] Intellectual property litigation is the source of nearly all large

61. The research methodology, including sample selection, for this database is explained in Rustad & Koenig, *supra* note 23. The statistical database was updated from the earlier study, but the methodology for collecting and examining the data is the same. As in the earlier study, coding decisions were often difficult in determining what constitutes a cybertort action. Many Internet-related cases, for example, included several causes of action. Spam-related cases invariably pleaded state and federal computer crime statutes in addition to the tort of trespass to chattels. Many intellectual property cases involved both the federal Lanham Act and a pendent tort cause of action. All cases were classified according to the central thrust or gravamen of the action. The analysis in Chart Three presents cases where the "predominant" cause of action was in tort or another substantive field. *See* Chart Three, *infra* p. 357.

62. We classify domain name disputes as intellectual property conflicts because the owners of trademarks file these lawsuits against domain name registrants. The FTDA applies when a website blurs a famous trademark by incorporating the mark in a domain name. 15 U.S.C. § 1125(c) (2000). Similarly, a domain name can tarnish a trademark, as in *Mattel, Inc. v. Jcom, Inc.*, 48 U.S.P.Q.2d (BNA) 1467, (S.D.N.Y. 1996), where the Barbie trademark was used on an adult entertainment web site. *Id.* at 1470. The court held that the use of the Barbie trademark combined with particular fonts and color schemes tarnished the mark. *See id.*; *see also* Hasbro, Inc. v. Internet Entm't Group, Ltd., No. C96-130WD, 1996 U.S. Dist. LEXIS 11626, at *2–3 (W.D. Wash. Feb. 9, 1996) (finding adult entertainment website tarnished distinctive mark of famous board game). In addition, trademark infringement may occur on the Internet when users of trademarks go to a domain name expecting to find sales or services provided by the trademark owner. People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 365–66 (4th Cir. 2001).

awards in cyberspace. For example, Sun Microsystems, Inc. recently agreed to pay Eastman Kodak $92 million to settle a patent infringement lawsuit over claims about Java technologies.[63]

Cyberlaw largely comprises disputes over maintaining and expanding the rights of service providers and other powerful stakeholders, rather than redressing the injuries, losses, or other damages suffered by consumers. Only eighteen percent of the Internet plaintiff victories were classified as mostly cybertort cases (N=99).[64] Many of the cybertorts arose out of intellectual property disputes. The business torts of unfair competition and misappropriation are often deployed in trade secret, as well as trademark, litigation.[65]

Thirteen percent of the cyberlaw cases were based on contract disputes in diverse actions such as wrongful termination cases, the failure to pay licensing fees, or the breach of fiduciary duty among investors in Internet start-ups (N=76).[66] Twelve percent of cases were based on constitutional or statutory grounds as opposed to common law. Most of these cases were filed against public school districts that disciplined students for improper postings on private websites. The students obtained relief on First Amendment grounds because the materials were protected speech.[67] The remaining few cases were Internet-related statutory causes of action, such as challenges to sexual offender registry law, the Electronic Communications Privacy Act (ECPA), and state use taxes.[68] The overwhelming conclusion is that

63. Jay Wrolstad, *Kodak, Sun Settle Java Patent Dispute*, NewsFactor Networks, *at* http://www.newsfactor.com/story.xhtml?story_title=Kodak—Sun-Settle-Java-Patent-Dispute&story_id=27459 (Oct. 8, 2004).

64. *See* Chart One, *supra* p. 352.

65. *See, e.g.*, 1-800 Contacts, Inc. v. WhenU.com, 309 F. Supp. 2d 467, 471, 509, 510 (S.D.N.Y. 2003) (granting injunction in copyright infringement, trademark infringement, and unfair competition action over use of domain name).

66. *See* Chart One, *supra* p. 352; *see, e.g.*, Tansey v. Trade Show News Network, Inc., C.A. No. 18796, 2002 WL 31521092, at *1–2 (Del. Ch. Oct. 28, 2002) (granting relief where outside investors were short-changed).

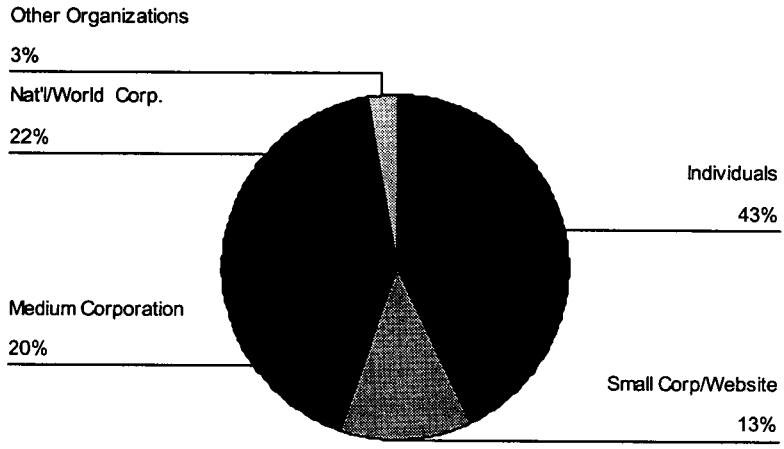
67. *See, e.g.*, Killion v. Franklin Reg'l Sch. Dist., 136 F. Supp. 2d 446, 448–49 (W.D. Pa. 2001) (granting summary judgment in favor of student where school disciplined student for anti-administration e-mail); Emmett v. Kent Sch. Dist. No. 415, 92 F. Supp. 2d 1088, 1089–90 (W.D. Wash. 2000) (granting temporary injunction against disciplinary action taken when student allowed visitors to website to vote on who would "die" next, that is, who would be subject of next mock obituary); Beussink v. Woodland R-IV Sch. Dist., 30 F. Supp. 2d 1175, 1177 (E.D. Mo. 1998) (enjoining school board from expelling student for inflammatory website).

68. Doe v. Dep't of Pub. Safety *ex. rel* Lee, 271 F.3d 38, 41 (2d Cir. 2001) (entering declaratory and permanent injunctive relief prohibiting state from disseminating information pursuant to Megan's Law); Urofsky v. Gilmore, 216 F.3d 401, 404 (4th Cir. 2000) (enjoining enforcement of

repeat players, in dramatic contrast to other classes of plaintiffs, have enjoyed great success in protecting their rights.

Chart Two

Type of Prevailing Cybertort Plaintiff



(Jan. 1992-July 2004) N=143

Chart Two substantiates the claim that intellectual property owners have benefited from a favorable legal environment in cyberspace. National, international, and medium-sized corporations were frequently plaintiffs, but they were far less likely to be defendants in cybertort cases. As shown in Chart Two, fifty-eight percent of the prevailing plaintiffs were corporations or other organizations that are likely to be repeat players.[69]

Virginia statute prohibiting state employees from accessing sexually explicit materials on computers owned or leased by state); McVeigh v. Cohen, 983 F. Supp. 215, 216–17 (D.D.C. 1998) (ruling that U.S. Navy violated plaintiff's rights under ECPA, APA, Navy policy, and Fourth and Fifth Amendments by intercepting e-mail in which plaintiff referred to his homosexuality).

69. AOL, for example, was the plaintiff in scores of anti-spam cases. *See, e.g.*, America Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 892 (N.D. Iowa 2001) (granting relief against unsolicited bulk e-mailers); America Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1268 (N.D. Iowa 2000) (denying AOL's summary judgment motion); America Online, Inc. v. CN Prods., Inc., No. CIV.A.98-552-A, 2002 U.S. Dist. LEXIS 1607, at *1 (E.D. Va. Feb. 10, 1999) (affirming discovery order in favor of AOL). Ford Motor Co. was another typical repeat player protecting its intangible assets in cyberspace. *See, e.g.*, Ford Motor Co. v. Catalanotte, 342 F.3d 543, 549 (6th Cir. 2003) (affirming that defendant "trafficked in" domain name

National or international corporations were successful plaintiffs in twenty-two percent of the 143 cybertort cases (N=31).[70] Medium-sized corporations and small corporations/websites comprised twenty percent (N=29) and thirteen percent (N=18) of the successful plaintiffs, respectively. This deployment of the legal system by formidable stakeholders "is not a new phenomenon, but has occurred throughout the twentieth century at times when technology outpaced the development of the law."[71]

Individuals are the leading type of successful plaintiffs, but their disputes tend to be with other individuals, not with corporate America or other commercial interests.[72] When individuals file cybertort lawsuits,

---

FordWorld.com within meaning of 15 U.S.C. § 1125(d) (2000) by offering to sell domain name to Ford Motor Co.); Ford Motor Co. v. Greatdomains.com, Inc., 177 F. Supp. 2d 635, 640–41 (E.D. Mich. 2001) (finding sufficient facts for cybersquatting claim in favor of Ford); Ford Motor Co. v. Lapertosa, 126 F. Supp. 2d 463, 464 (E.D. Mich. 2001) (finding danger of irreparable harm to plaintiff because Ford would have the ongoing burden of monitoring misappropriations of its trade secrets); Ford Motor Co. v. Ford Financial Solutions, Inc., 103 F. Supp. 2d 1126, 1129 (N.D. Iowa 2000) (finding trademark infringement for "colorable imitation" of Ford trademark in "financial services industry" and ordering defendant to assign domain name to international corporation); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 746, 754 (E.D. Mich. 1999) (dissolving temporary restraining order against website posting Ford's trade secrets). Mattel was also a repeat player, primarily suing to protect its trademarks and trade name. *See generally* Mattel, Inc. v. Antelman, No. 01 Civ. 8912 (LBS), 2002 U.S. Dist. LEXIS 1261 (S.D.N.Y. Jan 29, 2002); Mattel v. Adventurer Apparels, No. 00 Civ. 4085 (RWS), 2001 U.S. Dist LEXIS 13885 (S.D.N.Y. Sept. 7, 2001); Mattel v. Internet Dimensions, 55 U.S.P.Q.2d (BNA) 1620 (S.D.N.Y. July 13, 2000); Mattel, Inc. v. Jcom, Inc., 48 U.S.P.Q.2d (BNA) 1467 (S.D.N.Y. 1998).

70. *See, e.g.*, Cable News Network L.P. v. cnnews.com, 56 Fed. Appx. 599, 601 (Fed. Cir. 2003) (ordering in rem relief in domain name dispute against Chinese news company defendant); Eli Lilly & Co. v. Natural Answers, Inc., 233 F.3d 456, 459 (7th Cir. 2000) (entering preliminary injunction against dietary supplement manufacturer's "HERBROZAC" mark because it caused dilution which was element of FTDA); Caterpillar Inc. v. Telescan Techs., L.L.C., No. CIV.A.00-1111, 2002 U.S. Dist LEXIS 3477, at *8 (C.D. Ill. Feb. 13, 2002) (holding that infringer's verbatim incorporation of Caterpillar's marks in disputed domain names confused consumers); Caesar's World v. Caesarspalace.com, 112 F. Supp. 2d 502, 503 (E.D. Va. 2000) (finding in rem jurisdiction in favor of famous casino in cybersquatting case); AT&T Corp. v. Syntet, Inc., No. 96 C0110, 1997 U.S. Dist. LEXIS 1954, at *10, *39 (N.D. Ill. Feb. 11, 1997) (granting injunctive relief to AT&T in Internet-related trademark infringement case). The largest corporations also tend to be repeat players. One of the most frequent Internet litigants was Playboy Enterprises, which sued domain name registrants, cybersquatters, and other infringers. *See, e.g.*, Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1554, 1559, 1561 (M.D. Fla. 1993).

71. Bruce P. Keller, *Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property*, 11 HARV. J.L. & TECH. 401, 406 (1997).

72. *See, e.g.*, Bosley v. Wildwett.com, 310 F. Supp. 2d 914, 936 (N.D. Ohio 2004) (enjoining defendants from selling, distributing for sale, promoting for sale, or placing on "members only" websites any and all images of plaintiff); Griffis v. Luban, 646 N.W.2d 527, 536–37 (Minn. 2002) (refusing to enforce Alabama tort judgment against Minnesota resident for defamation and invasion

the causes of action are typically online defamation, employment-related torts, or, to a lesser extent, the invasion of privacy. Punitive damages awards to cybertort plaintiffs usually arise out of incendiary interpersonal disputes carried out on the Internet. In more than a decade of cyberlaw litigation, only one consumer won a legal or equitable remedy against a company in an Internet-related commercial transaction.[73] Large corporations are less likely to be sued because they enjoy § 230 immunity. ISPs are in the enviable position of being repeat players who use litigation to extend their rights and remedies, while being immunized from lawsuits by consumers and other computer users.

Individuals and small companies were the most likely to suffer defeat in these lawsuits. Nearly half of the unsuccessful defendants (48%, N=68) were startup e-commerce companies, spam e-mailers, cybersquatters, websites, or other small companies. One in four cases involved individual defendants (N=35). Medium-sized companies were defendants in only 13 percent of the cases (N=18), followed by nationally or internationally known corporations (11%, N=6). The remaining six defendants were other entities (4%).

C. *Most Cybertorts Involve Disputes over Intellectual Property*

Intellectual property disputes predominate in cyberspace because service providers and other content providers are also content creators interested in protecting and extending their rights. As America evolves from a durable goods economy to an information-based one, torts are shifting from accident law to protecting corporate stakeholders from infringement of their intellectual property rights. The Internet is being enclosed by "legally backed digital fences, lengthened copyright terms and increased penalties."[74] Repeat players utilize common law-based remedies,[75] as well as federal statutes to protect their intellectual

---

of privacy for statements made by Minnesota resident on Internet).

73. The case, Freeman *ex rel* Mortgage.com v. Levine, No 00-322262-CA-03 (Fla. Miami-Dade County Ct. filed Aug. 10, 2001), involved suit against eleven of Mortgage.com's top management officials for online financial fraud and breach of fiduciary duty. *See* Matthew Hagman, *Verdicts and Settlements 06.23.03*, DAILY BUS. REV., at 1, *available at* http://delaomarko.com/_private/newspages/MDCM%20Business%20Review%2006.23.03.pdf (last visited Apr. 24, 2005). On June 13, 2003, the parties settled for $4.7 million. *Id.*

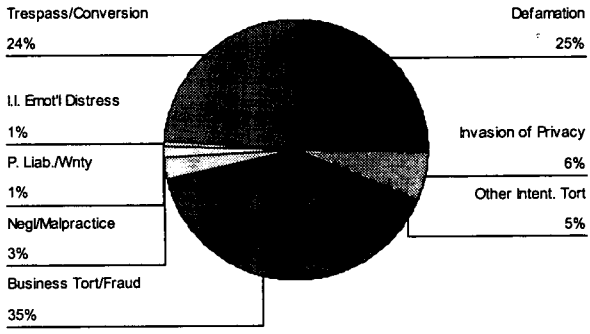
74. James Boyle, *Foreword: The Opposite of Property?*, 66 LAW & CONTEMP. PROBS. 1, 1 (2003) (quoting Jerry Reichman and David Lange).

75. At common law, the infringement of intellectual property rights had its genesis in the law of torts. Keller, *supra* note 71, at 406.

property.[76]

Chart Three

Cause of Action in Internet Torts



(Jan. 1992-July 2004) N=143

Individuals who prevail as plaintiffs in cyberspace litigation generally allege reputational, privacy, or financial injuries against other individuals or entities, in sharp contrast to the largely personal injury docket of traditional tort law. No plaintiff has won a case based on claims that he or she suffered personal injury in cyberspace from the negligent acts of repeat players. To date, for example, no online patient has recovered damages based on an injury arising from the practice of telemedicine.[77] No computer professional has been held liable for professional negligence in an Internet case, even though there is an epidemic of security breaches due to bad software.[78] No actions for defective software, Internet security services, or computer products have been successful.

Almost all Internet cases involve plaintiffs seeking redress for

76. Novell, for example, aggressively employs its patent portfolio, and thus federal patent law, as a principal means to defend its open-source software and proprietary offerings against e-patent attacks. Jay Wrolstad, *Novell Pledges to Protect Open Source Against Legal Claims*, *at* http://www.newsfactor.com/story.xhtml?story_id=27606 (Oct. 14, 2004); *see* 35 U.S.C. §§ 101–103 (2000) (establishing conditions for patentability of inventions).

77. "The Institute of Medicine has defined telemedicine to encompass telephone, video and electronic transmission of medical information using telephone or digital technology." Alissa R. Spielberg, *Online Without a Net: Physician–Patient Communication by Electronic Mail*, 25 AM. J.L. & MED. 267, 287–88 (1999).

78. *See* Thomas G. Wolpert, *Product Liability and Software Implicated in Personal Injury*, 60 DEF. COUNSEL J. 519, 521 (1993).

financial loss or injury to reputation. Personal injury or property damage cyberspace claims have yet to evolve, and therefore there have been no damage awards for physical pain, mental suffering, disability, disfigurement, or loss of enjoyment of life. In sharp contrast, a U.S. Department of Justice study of tort cases in large U.S. counties revealed that ninety-two percent of traditional state tort cases involved personal injury caused by negligent or intentional acts.[79]

Few personal injury actions are filed in Internet-related cases because of the lack of successful precedent. U.S. courts have been slow to recognize any negligence-based actions in cyberspace. Perhaps the most significant reason for the paucity of personal injury-based cybertorts is that the plaintiff does not typically suffer a clear-cut physical injury from surfing the Web. When an individual is victimized in cyberspace, it is generally an information-based injury, such as loss of reputation, invasion of privacy, or fraud.

In the brick-and-mortar world, negligence-based cases dominate the legal landscape.[80] The most frequent type of traditional tort case involves an individual suing another individual (47%), followed by an individual suing a business (37%).[81] The universe of Internet torts, in sharp contrast, continues to be doctrinally rooted in personal property torts that originated during England's feudal period, such as conversion and trespass to chattels. An astonishing 101 of the 143 cybertort plaintiffs (71%) based their claims on intentional torts.[82] In our sample, plaintiffs in only four cases asserted negligence or malpractice causes of action. Corporations, rather than individual litigants, filed three-quarters of the cybertort cases in which negligence was at issue.

Business tort or fraud cases arising out of e-commerce dominated the cyberspace docket. Intentional business torts, such as fraud or misrepresentation, intentional interference with contract, unfair competition, or the misappropriation of trade secrets, composed the single largest category of intentional torts (35%, N=50).[83] Thirty-six out

79. SMITH ET AL., *supra* note 60, at 1–2.

80. The U.S. Department of Justice study of tort cases in large U.S. counties concluded that the majority of cases disposed were automobile torts. *Id.* at 1. Only one in ten cases involved more complex litigation such as medical malpractice, products liability, or toxic torts litigation. *Id.*

81. *Id.* at 5.

82. The intentional torts that we included were trespass to chattels/conversion, intentional infliction of emotional distress, business torts/fraud, and miscellaneous intentional torts. *See* Chart Three, *supra* p. 357.

83. *See* Chart Three, *supra* p. 357.

of the fifty business tort cases or fraud cases were filed by corporate entities. Medium to large corporations filed almost half of the business tort cases (twenty-three out of fifty).

In more than a decade of Internet cases, only one company has been forced by a court to make any restitution for the sale of defective goods on its website.[84] This sole successful products liability action, a 2003 case, arose out of the website sale of a field-monitoring device for tracking criminals under house arrest.[85] The manufacturer's website advertised that its field-monitoring unit in the offender's home would detect any tampering.[86] However, when a murderer cut off the ankle device, he was out of range of the monitoring unit, so the home unit did not detect the tampering.[87] The court refused to impose a legal duty on the manufacturer to make a tamper-proof field-monitoring device.[88] Similarly, the court found that the monitoring device did not breach any express or implied warranty, nor was it defectively manufactured.[89] The victim's estate successfully brought an action only for misrepresentation based on false statements about the field-monitoring unit on the company's website.[90]

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.[91] A typical example is *America Online, Inc. v. National*

84. Kirby v. B.I. Inc., No. CIV.A.4:98-CV-1136-Y, 2003 U.S. Dist. LEXIS 16964, at *49–50 (N.D. Tex. Sept. 26, 2003).

85. *Id.* at *2–16.

86. *Id.* at *19.

87. *Id.* at *20.

88. *Id.* at *37 (ruling that manufacturer did not have design defect in its security bracelet because it was not feasible to produce tamper-proof product).

89. *Id.* at *42 (ruling that there was no express warranty because no representations were made to plaintiff); *id.* at *44 (ruling that field monitor device or security bracelet was merchantable in that it was fit for ordinary purposes for which devices were used).

90. *Id.* at *19–20 (ruling that public representations made by company on its website were false and misleading).

91. For the period of 1992–2002, there were 114 cybertort cases. In the earlier research, twenty-seven percent [N=31] of the cybertort cases involved defamation or injurious falsehood claims. The four most common Internet-related actions were business torts (35%, [N=40]), personal property torts, including trespass to chattels or conversion (28%, [N=32]), and online defamation (27%, [N=31]). Ninety-seven percent of the 114 cybertorts were intentional tort cases, in contrast to the negligence cases dominating traditional caseloads. Rustad & Koenig, *supra* note 23, at 93.

Health Care Discount, Inc.,[92] in which the ISP deployed the ancient tort of trespass to chattels against a spam e-mailer.[93] The court gauged compensatory damages by charging the spammer $2.50 per thousand unwanted e-mails, for a total of $337,500.[94] Perhaps the most high profile cyber-conversion case arose out of the fraudulent conversion of the Sex.com domain name.[95] In that case, the trial court levied a $65 million judgment against a pornographer.[96] However, the plaintiff is unlikely to collect this award because the defendant fled to an off-shore venue to escape the judgment.[97]

Online defamation cases accounted for one in four cybertort cases, and it is in this substantive field of tort law that individuals predominate.[98] The defendants in these cases were almost all individuals, rather than online businesses or providers. Twenty-eight of the thirty-six winning online defamation cases involved individuals suing other individuals. The few non-individual claims arose out of false or defamatory statements about business practices that were published on websites.[99] A telecommunications company, for example, filed a

92. 174 F. Supp. 2d 890 (N.D. Iowa 2001).

93. *Id.* at 893.

94. *Id.* at 901.

95. Kremen v. Cohen, 337 F.3d 1024, 1026–27 (9th Cir. 2003) (affirming judgment of federal district court as to claims for breach of contract, and breach of third-party contract, but reversing ruling that domain names, although a form of property, were intangibles not subject to conversion).

96. *Id.* at 1027; Laurie Flynn, *Cybersquatting Draws Heavy Penalty*, N.Y. TIMES, Apr. 6, 2001, at C6.

97. "Although Kremen got vindication of the legal win, he has not been able to collect money from Cohen, who is wanted on a warrant for not appearing in court." Michael Bartlett, *Right to a Domain Name at Issue in Sex.com Case*, *at* http://www.findarticles.com/p/articles/mi_m0NEW/is_2002_Feb_20/ai_83087547 (Feb. 20, 2002). While the primary defendant defaulted, Verisign recently settled the case with Sex.com. Dawn Kawamoto, *Sex.com, VeriSign Settle Domain Name Suit, available at* http://news.com.com/2100-1038_3-5195669.html (April 20, 2004).

98. Courts vary in defining defamation, and often a particular definition or rule is peculiar to a small number of jurisdictions. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 111, at 773 (5th ed. 1984). Defamation is "that which tends to injure 'reputation' in the popular sense; to diminish the esteem, respect, goodwill or confidence in which the plaintiff is held, or to excite adverse, derogatory or unpleasant feelings or opinions against him." *Id.* Keeton describes the prima facie case as follows:

> it has always been necessary for the plaintiff to prove as a part of his prima facie case that the defendant (1) published a statement that was (2) defamatory (3) of and concerning the plaintiff. In a typical case of defamation, the publisher (1) realized that the statement made was defamatory, (2) intended to refer to the plaintiff, and (3) intended to communicate it to a third person or persons.

Id. § 113, at 802.

99. A business defamation lawsuit occurs when an untrue statement is communicated which

business defamation action against defendants who posted negative messages about its corporate practices.[100]

Because corporations have no right to privacy, it is not unexpected that all of the privacy-based cybertort cases involved individuals suing their neighbors, employers, or strangers (N=9). Similarly, the only intentional infliction of emotional distress case was filed on behalf of an individual against another individual. The rarity of emotional distress cases is notable considering that the Internet can readily be used as a tool of sexual harassment and other forms of gender discrimination.[101]

Intentional torts, for the most part information-based and personal property litigation, have evolved, but, as Chart Three reveals, there are almost no successful actions for negligence or strict liability. Traditional tort law evolved in response to industrial or automobile accidents that caused death or permanent disability.[102] The law of cybertorts has been too slow to extend the concepts of products liability[103] to cyberspace.[104] No personal injury or wrongful death claims have resulted in plaintiff's victories, even in the most recent period of cyberspace litigation.

"prejudice[s] [the business entity] in the conduct of its business and deter[s] others from dealing with it." A.F.M. Corp. v. Corp. Aircraft Mgmt., 626 F. Supp. 1533, 1551 (D. Mass. 1985); *see, e.g.*, Amway Corp. v. Proctor & Gamble Co., 1:98-CV-726, 2000 U.S. Dist. LEXIS 372, at *15–16 (W.D. Mich. Jan. 6, 2000) (ruling that Amway made prima facie showing that P & G's web site was aimed at forum and caused harm to its business reputation).

100. Global Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d 1261, 1263 (C.D. Cal. 2001) (granting defendant's motion to dismiss on grounds that California's Anti-SLAPP (Strategic Litigation Against Public Participation) provisions applied and defendant's postings about company were protected as exercise of free speech in connection with public issue); *see also* Media3Technologies, LLC v. Mail Abuse Prevention Sys., LLC, 00-CV-12524-MEL, 2001 U.S. Dist. LEXIS 1310, at *2 (D. Mass. Jan. 2, 2001) (dismissing business defamation or trade libel claim against web host that argued its business reputation had been injured by being placed on ISP's "black-hole list").

101. *See* Rustad & Koenig, *supra* note 23, at 128–29.

102. KOENIG & RUSTAD, *supra* note 52, at 29–37 (discussing period from 1825 to 1894 as negligence era in American tort law).

103. The field of products liability refers to rights and remedies to redress personal injuries and economic losses caused by defective products. "Products liability is the name currently given to the area of the law involving the liability of those who supply goods or products for the use of others to purchasers, users, and bystanders for losses of various kinds resulting from so-called defects in those products." KEETON ET AL., *supra* note 98, § 95A, at 677. It is unclear whether the concept of products liability can be extended to defective information on websites. Nathan D. Leadstrom, *Internet Web Sites as Products Under Strict Products Liability: A Call for an Expanded Definition of Product*, 40 WASHBURN L.J. 532, 534 (2001).

104. In the earlier study that this Article updates, there were "no products liability or warranty actions and only a trivial number of negligence-based cases." Rustad & Koenig, *supra* note 23, at 113.

Personal injury or death claims are rarely based on website activity. Most tort injuries are financial injuries; reputation damage; or the unauthorized theft of trade secrets, privacy, or other information-based losses. The injury problem in cyberspace is based on intangible losses, unlike the disfigurement or pain and suffering experienced by the victims of physical injury. Nevertheless, these economic or information-based injuries are legally protectable interests.

In summary, the current cybertort landscape protects dominant repeat players while leaving consumers with little or no protection for financial injuries, the loss of privacy and identity, and other information-based intrusions or losses. Unlike traditional brick-and-mortar torts that focus on personal injuries, cybertorts have yet to evolve to provide remedies for information-based torts outside of the narrow band of intentional torts used by the business community. This lopsided progression of cybertort law has left consumers with an injury problem in cyberspace.

II. THE PATH OF CYBERTORT LAW

> *The Internet's pace of adoption eclipses all other technologies that preceded it. Radio was in existence 38 years before 50 million people tuned in; TV took thirteen years to reach that benchmark. Sixteen years after the first PC kit came out, 50 million people were using one. Once it was opened to the general public, the Internet crossed that line in four years.*[105]

This Part traces the pathways of cyberspace legal precedents that explain our empirical finding that most cybertorts are stillborn. Courts have stretched § 230 excessively, protecting ISPs against distributor liability and almost every other tort cause of action.[106] This bloating of ISP immunity to encompass most torts has resulted in a legal environment that is contrary to the interests of consumers and other Internet users.

The expansive immunity given to ISPs by § 230 has "transform[ed]

105. U.S. DEP'T OF COMMERCE, THE EMERGING DIGITAL ECONOMY 4 (1998).

106. Courts have expanded the meaning of 47 U.S.C. § 230(f)(2) (2000) to include a wide range of Internet services, not just ISPs. For example, a court found eBay's online auction service was entitled to protection under § 230. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 714 n.7 (2002) (defining eBay as "interactive computer service provider" within meaning of § 230). Similarly, a Washington State court classified Amazon.com's online bookstore as an interactive computer service provider. *See* Schneider v. Amazon.com, Inc., 108 Wash. App. 454, 460–63, 31 P.3d 37, 40–41 (2001).

the Internet into an almost liability-free zone for libelous content."[107] The most dominant online intermediaries enjoy unlimited immunity while the principal tortfeasor is generally judgment-proof or inaccessible by legal process. This unhinged legal environment creates "considerable harm not only to those whose reputations and livelihood are endangered by libelous statements, but also to the potential of the Internet as a reliable, easily accessible, and inexpensive means of communication."[108]

A. Pre-CDA Cybertort Developments

> *The law embodies the story of a nation's development through many centuries . . . . In order to know what it is, we must know what it has been, and what it tends to become.*[109]

Oliver Wendell Holmes drew upon more than six centuries of common law development in his renowned 1897 lecture, "The Path of the Law."[110] He wrote during a period of revolutionary tort law development, which had been impelled by advances in transportation and communication technologies. Prior to the late nineteenth century, the law of torts was fundamentally about defending community tranquility.[111] In the nineteenth century, the law of negligence progressed to provide remedies for mass accidents caused by broken-down rail trestles, slipshod maintenance of tracks, or reckless operation of trains.[112] When Justice Holmes gave his legendary address, privacy-based torts, along with remedies for misuse of novel technologies such as

---

107. Christopher Butler, *Plotting the Return of an Ancient Tort to Cyberspace: Towards a New Federal Standard of Responsibility for Defamation for Internet Service Providers*, 6 MICH. TELECOMM. & TECH. L. REV. 247, 248 (2000).

108. *Id.*

109. OLIVER WENDELL HOLMES, THE COMMON LAW 1 (Little, Brown & Co. 1945) (1881).

110. *See generally* OLIVER WENDELL HOLMES, *The Path of the Law*, *in* COLLECTED LEGAL PAPERS 167 (1920).

111. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 974–78 (1989) (arguing that law of torts reflects community norms).

112. In an earlier article, one of the Authors elaborated:

> Before there were mega cases, there was mega death from mass disasters, such as railroad or industrial accidents. The law of torts entered the negligence era "around the turn of the nineteenth century as turnpikes and burgeoning industry were vastly accelerating the pulse of activity and confronting society with an accident problem of hitherto unprecedented dimensions."

Michael L. Rustad, *Smoke Signals from Private Attorneys General in Mega Social Policy Cases*, 51 DEPAUL L. REV. 511, 534 (2001) (footnote omitted).

"instantaneous photographs," were being born.[113]

In the new millennium, American society is once again undergoing a technological conversion of great consequence. This time, America is evolving from a durable commodities-based economy to one based on the licensing of software, intellectual property, and other intangibles. To trace the path of Internet law, we need only review a decade and a half of legal precedents.

An Internet fraudster once claimed that his company "will either develop a machine itself or be so well known that a traveler from the future will go back in time and provide the company with the technology to develop the time machine."[114] If time could be suddenly turned back to 1990 and you were to look about you, what would seem extraordinary about the ascendancy of the Internet? To begin with, the World Wide Web had yet to be invented,[115] and most international corporations did not have websites or require their employees to have e-mail accounts.

A time-traveler would be an eyewitness to the early 1990s, when conflicts or cyberspace rights first became a legal issue. In 1990, a federal court mentioned the term "Internet" for the first time.[116] That year also witnessed the first criminal conviction of a computer hacker, who broke into Bell South's 911 computer files.[117] The first cybertort case was decided in 1991, when CompuServe, Inc. was held not liable for a third party's publication of defamatory statements on its services.[118] In 1991, the United States Court of Appeals for the Third Circuit struck down a one-sided shrink-wrap license agreement, holding that Article 2

113. *See* MADELEINE SCHACHTER, INFORMATIONAL AND DECISIONAL PRIVACY 3 (2003) (attributing conceptualization of privacy as right to be left alone to THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (Chicago, Callaghan 1879)). *See generally* Warren & Brandeis, supra note 30.

114. John Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, 74 IND. L.J. 893, 917 n.96 (1999) (describing fraudulent Internet sale of investments in time machine).

115. Tim Berners-Lee developed the World Wide Web at CERN in Switzerland in 1991. It was not until the mid-1990s that the World Wide Web reached its takeoff point. *See* Ben Segal, *A Short History of Internet Protocols at CERN, at* http:/wwwinfo.cern.ch/pdp/ns/ben/TCPHIST.html (Apr. 1995).

116. United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991) (upholding conviction of creator of Internet worm that caused interconnected university computers to crash).

117. United States v. Riggs, 743 F. Supp. 556, 558 (N.D. Ill. 1990) (upholding convictions for wire fraud as well as for violations of Computer Fraud and Abuse Act of 1986, Pub. L. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2000))).

118. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 137, 140 (S.D.N.Y. 1991) (ruling that ISP was not publisher and was therefore analogous to mere conduit such as newsstand or bookstore).

of the Uniform Commercial Code applied to software.[119]

The domain name registration system began to go forward in 1992, when the National Science Foundation entered into a contract with Network Solutions, Inc. to develop registration procedures.[120] In 1993, a federal court became the first to hold a website liable for copyright and trademark infringement for unauthorized distribution of photographs on an Internet bulletin board.[121] The next year, a court held for the first time that mere access to a database in another state was insufficient basis for personal jurisdiction.[122]

Since the mid-1990s, parties have litigated thousands of disputes over trademarks in cyberspace. The first clash between a domain name registrant and a trademark owner was decided only a decade ago.[123] In 1994, a court held an electronic bulletin board service liable for contributory copyright infringement for operating a website where users could download copyrighted video games at no cost.[124] Internet law historians would surely agree that all of cyberspace legal history has belonged to the powerful online stakeholders. If Hollywood produced a film of the history of Internet law, it would be entitled, "Honey, We've Shrunk the Commons!"[125] The Internet has been used to broadcast medical images, videos, and provide medical consultations for more than a decade, yet no tort of telemedicine has evolved. Computerized records made it possible for financial institutions to provide synchronized access to far-flung users. Yet there is no case law on the duty of online companies to protect privacy. Attorneys habitually transmit confidential client data on the Internet, but there have been no tort actions where information was intercepted.

In the early years of the World Wide Web, it was not apparent how existing tort law would pertain to online commerce. *Cubby, Inc. v.*

---

119. Step-Saver Data Sys., Inc., v. Wyse Tech., 939 F.2d 91, 99 (3d Cir. 1991) (refusing to enforce shrink-wrap agreement on grounds that it violated UCC § 2-207's battle of the forms provision).

120. Antony J. McShane & Orrin S. Shifrin, *Protecting Trademarks and Copyrights in the New Millennium*, 14 CBA REC. 32, 32 (Apr. 2000).

121. Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1554, 1559, 1561 (M.D. Fla. 1993).

122. Pres-Kap, Inc. v. Sys. One, Direct Access, Inc., 636 So. 2d 1351, 1353 (Fla. Dist. Ct. App. 1994).

123. *See generally* MTV Networks v. Curry, 867 F. Supp. 202 (S.D.N.Y. 1994).

124. Sega Enters. Ltd. v. Maphia, 857 F. Supp. 679, 689, 690 (N.D. Cal. 1994).

125. *See generally* Thomas L. Friedman, *Honey, I Shrunk the World*, N.Y. TIMES, Sept. 12, 1999, § 4, at 19.

CompuServe Inc.,[126] was the first cybertort case where a court considered whether an ISP was a publisher or distributor for purposes of defamation law.[127] CompuServe's bulletin board hosted an electronic newsletter called "Rumorville USA."[128] The plaintiff began publishing a rival online publication he called "Skuttlebut."[129] One of CompuServe's subscribers posted a statement on Rumorville dismissing the competing publication as a "start-up" swindle.[130] The creator of Skuttlebut filed a defamation action against Rumorville and CompuServe on the theory that it was a republisher of defamatory content.[131] CompuServe filed a motion to dismiss, arguing that it was a distributor without constructive or actual knowledge of the defamatory communiqué on its bulletin board.[132] CompuServe contended that, because it lacked any opportunity to screen content, it was a mere distributor.[133]

The *Cubby* court held that CompuServe exercised no editorial control over materials on its bulletin boards and was therefore a distributor for purposes of the law of defamation.[134] Because CompuServe had neither actual nor constructive notice of the defamatory content on Skuttlebut, it had no liability.[135] In the wake of *Cubby*, ISPs had a reasonable expectation that courts would classify them as distributors for third party content posted on their services.

126. 776 F. Supp. 135 (S.D.N.Y. 1991).

127. *Id.* at 139.

128. *Id.* at 137.

129. *Id.* at 138.

130. *Id.*

131. *Id.* at 139.

132. *Id.*

133. The court stated:

> CompuServe has no opportunity to review Rumorville's contents before DFA uploads it into CompuServe's computer banks, from which it is immediately available to approved CIS subscribers. CompuServe receives no part of any fees that DFA charges for access to Rumorville, nor does CompuServe compensate DFA for providing Rumorville to the Journalism Forum; the compensation CompuServe receives for making Rumorville available to its subscribers is the standard online time usage and membership fees charged to all CIS subscribers, regardless of the information services they use. CompuServe maintains that, before this action was filed, it had no notice of any complaints about the contents of the Rumorville publication or about DFA.

Id. at 137.

134. The court was persuaded that CompuServe was a distributor because it exercised almost no editorial control over anything posted on its message boards or electronic bulletin boards. *Id.* The federal court reasoned that, because it exercised no control, it could only be liable for torts if the plaintiff proved that the ISP had actual or constructive knowledge of defamatory materials. *Id.* at 141.

135. *Id.* at 141.

The 1995 case of *Stratton Oakmont, Inc. v. Prodigy Services Co.*[136] muddied the path of cybertort law. Like *Cubby*, this defamation case originated from an online denunciation posted on an electronic bulletin board. One of Prodigy's subscribers posted a message accusing Stratton Oakmont of fraudulent security offerings.[137] Stratton Oakmont sued the ISP, demanding $100 million in punitive damages for the cyberslur.[138] The *Stratton Oakmont* court ruled that Prodigy could be held liable for defamatory statements made by its subscribers because it was fulfilling the classic role of a publisher by screening and preparing content for its users.[139]

The dissimilar rulings in *Cubby* and *Stratton Oakmont* may be partially explained by the difference in the services that these ISPs provided to their customers. During the early 1990s, Prodigy carved out a niche in the Internet mass market by advertising that it offered a safe Internet that was suitable for family use.[140] Prodigy filtered out objectionable material and monitored the content on its computer bulletin boards to promote its family-oriented services.[141] In contrast, CompuServe did not screen for pornographic or other objectionable content.[142]

Prodigy's gatekeeper role[143] in detecting and screening out objectionable content made it more vulnerable to claims that it was a publisher than ISPs like CompuServe that made no effort to screen out denigrating or even dangerous content. The parties settled the *Prodigy* case on October 24, 1995, while an appeal was pending, so the opinion

136. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

137. *Id.* at *1.

138. *Id.*

139. *Id.* at *4.

140. When Prodigy began its services in 1990, it held itself out as a:

> family oriented computer network. In various national newspaper articles written by Geoffrey Moore, Prodigy's Director of Market Programs and Communications, Prodigy held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and expressly likening itself to a newspaper.

Id. at *2.

141. *Id.*

142. CompuServe, Inc. made no effort to monitor content or provide any editorial services. It loaded text and databases instantaneously without any means to filter out objectionable content. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991).

143. Professors Mann and Winn use the term "gatekeeper liability" to describe the potential liability an ISP intermediary risks for failing to constrain cyberinfringers, cybercriminals, and cybertortfeasors. *See* MANN & WINN, *supra* note 9, at 188–89.

has no precedential value.[144] Stratton Oakmont agreed not to contest Prodigy's motion to request that the court reverse or set aside its prior ruling that the ISP was a publisher for purposes of defamation law.[145]

As demonstrated by the *Cubby* and *Stratton Oakmont* cases, the common law created a perverse incentive by punishing ISPs that attempted to protect their subscribers from torts and crimes with liability as a publisher,[146] while ISPs that did nothing to prevent crimes and torts were classified as distributors and received limited liability.[147] Dissatisfied with this result, ISPs successfully lobbied Congress to enact an across-the-board federal immunity that supplanted state defamation law. In 1996, Congress, through the CDA, expressly overruled *Prodigy* by immunizing all online intermediaries from publisher's liability.[148] Congress enacted the CDA to prevent the newborn industry of ISPs from drowning in a sea of litigation.[149]

B. The Communications Decency Act

Section 230 of the CDA was a dream come true for ISPs: Congress made it clear that no interactive computer service would be classified as a publisher or speaker so long as third parties had provided the content.[150] The legislative purpose of § 230(b) was to "promote the continued development of the Internet" and "to preserve the vibrant and competitive free market that presently exists . . . unfettered by Federal or State regulation."[151] When Congress passed § 230, it recognized that the Internet provides Americans with "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[152] While creating protections for Internet users, Congress sought to preserve these positive attributes and discourage excessive regulation that might restrain the Internet's

144. Peter H. Lewis, *After Apology from Prodigy, Company Drops Suit*, N.Y. TIMES, Oct 25, 1995, at D1.

145. *Id.*

146. *Stratton Oakmont, Inc.*, 1995 WL 323710, at *4.

147. *Cubby, Inc.*, 776 F. Supp. at 137.

148. 47 U.S.C. § 230 (2000).

149. *See id.* § 230(c)(1) (stating, "[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider").

150. *Id.*

151. *Id.* § 230(b).

152. *Id.* § 230(a)(3).

development.[153]

By immunizing websites from publisher liability claims, Congress's enactment of § 230 of the CDA left the victims of defamation without any meaningful remedy. The common law divided potential defamation defendants into three categories: "as primary publishers (such as book or newspaper publishers); as conduits (such as a telephone company); or as distributors (such as a book store, library, or news dealer)."[154] Under the common law of defamation, publishers have maximum exposure to defamation liability as content providers.[155] The common law of defamation distinguishes between primary publishers and secondary distributors of information. Distributors or secondary disseminators, such as libraries, newsstands, or bookstores, are not liable for defamation based on objectionable content absent "proof that they knew or had reason to know of the existence of defamatory matter" contained in the product they distribute.[156]

It would be "rather ridiculous, under most circumstances, to expect a bookseller or a library to withhold distribution of a good book because of a belief that a derogatory statement contained in the book was both false and defamatory . . . ."[157] A bookstore, for example, "simply assists primary publishers in distributing information."[158] Thus, distributors enjoy limited protection because they are not content creators. In contrast, "[p]ublishers can be held liable for defamatory statements contained in their works even absent proof that they had specific

153. *Id.* § 230(b)(1)–(2).

154. Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 166–67 (Cal. Ct. App. 2004), *review granted and opinion superseded by* 87 P.3d 797 (Cal. 2004).

155. Traditional defamation law

> categorized information disseminators into three groups to which very different legal standards were applied to determine defamation liability related to third-party content: (1) publishers (e.g., newspapers) exercise great control over final content and were therefore subject to strict liability; (2) distributors (e.g., booksellers) merely distribute content and were therefore subject to liability only upon a showing of knowledge or negligence; and (3) common carriers (e.g., telephone companies) only transmit information with no control over content and were therefore not liable at all.

Jae Hong Lee, Note, Batzel v. Smith *&* Barrett v. Rosenthal*: Defamation Liability for Third-Party Content on the Internet*, 19 BERKELEY TECH. L.J. 469, 471 (2004); *see, e.g.*, Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991) (explaining broader liability of publishers who are treated as content creators versus distributors who are only liable if they have knowledge of defamatory content).

156. KEETON ET AL., *supra* note 98, §113, at 811.

157. *Id.*

158. *Id.*

knowledge of the statement's inclusion."[159]

Because courts have interpreted § 230 to provide ISPs with both publisher and distributor immunity,[160] an ISP has no duty to perform any investigation before posting or reposting tortious material and disseminating it around the world. An ISP could, for example, receive an e-mail from an unknown source containing obviously defamatory statements and post it on its website without fear of liability. Even if the content was clearly tortious on its face, the message would be classified as "information provided by another information content provider" for purposes of § 230 immunity.[161] Similarly, the moderator of a listserv or the operator of a website who posts an allegedly defamatory e-mail authored by a third party will not be held liable.[162]

At present, the targets of consumer fraud or other online injuries have no recourse against ISPs or other online intermediaries, even if the service provider has actual knowledge of ongoing torts or crimes on its services. Courts have flatly refused to strip CDA immunity even when the ISP has an active role in creating or distributing the content.[163]

As a result of § 230, AOL, CompuServe, and Prodigy are immunized from publisher's liability so long as third parties create the content.[164] The immunity from publisher liability granted by § 230 of the CDA has continuing vitality a decade after its passage.[165] The development of the

159. KEETON ET AL., *supra* note 98, § 113, at 810.

160. *See, e.g.*, Zeran v. America Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (stating that publishers and distributors are identical for purposes of defamation law); Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 166–67 (Cal. Ct. App. 2004) (conferring immunity on ISP for distributor liability), *review granted and opinion superseded by* 87 P.3d 797 (Cal. 2004).

161. The CDA defined an "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3) (2000).

162. *See* Batzel v. Smith, 333 F.3d 1018, 1031–35 (9th Cir. 2003).

163. For example, in *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998), the court conferred CDA immunity on AOL for defamation liability, despite the fact that AOL had a written license agreement with Matt Drudge in which AOL agreed to pay him to produce content for the service. *Id.* at 51–52. "The agreement made the Drudge Report available to all members of AOL's service for a period of one year. In exchange, defendant Drudge received a flat monthly 'royalty payment' of $3,000 from AOL. During the time relevant to this case, defendant Drudge has had no other source of income." *Id.* at 47. AOL also set the terms for Drudge's creation, editing, and management of the online Drudge report. *Id.*

164. In passing § 230, "Congress decided not to treat providers of interactive computer services like other information providers such as newspapers, magazines or television and radio stations, all of which may be liable for publishing or distributing obscene or defamatory material written or prepared by others." *Id.* at 49.

165. The CDA immunity parallels the nineteenth century legal subsidies that insulated the railroad, steamboat companies, canal builders, and other builders of the nineteenth century industrial

Internet would have been crippled without this legal shield. Too much tort liability propagates widespread online censorship, which would greatly impede freedom of expression on the Internet.

An activist judiciary, however, has radically expanded § 230 by conferring immunity on distributors.[166] Section 230(c)(1) has been interpreted to preclude all tort lawsuits against ISPs, websites, and search engines.[167] Courts have extended the meaning of "interactive computer services,"[168] haphazardly lumping together web hosts, websites, search engines, and content creators into this amorphous category.[169] Federal and state courts have immunized providers from the torts of third parties predicated on the invasion of privacy,[170] negligence,[171] negligent misrepresentation,[172] defamation,[173] distributor liability,[174] intentional

---

economy. *See* MORTON HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1780–1860, at 99–101 (1977).

166. *See* Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 166–67 (Cal. Ct. App. 2004), *review granted and opinion superseded by* 87 P.3d 797 (Cal. 2004).

167. RUSTAD & DAFTARY, *supra* note 49, § 5.02[B][2][a], at 5–26 (reporting § 230 cases where courts expanded immunity for providers).

168. Batzel v. Smith, 333 F.3d 1018, 1020 (9th Cir. 2003).

169. *See, e.g.*, Doe v. GTE Corp., 347 F.3d 655, 659, 663 (7th Cir. 2003) (affirming dismissal of tort claim that web host aided and abetted sale of secretly obtained video tapes showing undressed athletes); *Batzel*, 333 F.3d at 1031, 1034–35 (holding that website operator fell within immunity of § 230, but remanding issue of whether defamatory e-mail was meant to be posted on listserv); Ben Ezra, Weinstein, & Co. v. America Online, Inc., 206 F.3d 980, 985 (10th Cir. 2000) (holding Internet access provider was immunized for providing access to misleading stock information); OptInRealBig.com, LLC v. IronPort Sys., Inc., 323 F. Supp. 2d 1037, 1047 (N.D. Cal. 2004) (denying injunction in favor of spam e-mailer, ruling that spam complaint website was immunized from liability under CDA); Ramey v. Darkside Prods., No. CIV.A.02-730 (GK), 2004 U.S. Dist. LEXIS 10107, at *12–21 (D.D.C. May 17, 2004) (ruling that online advertising guide for adult entertainment was immunized by CDA in claim by woman that unauthorized photos were used on advertisement on website); PatentWizard, Inc. v. Kinko's, Inc., 163 F. Supp. 2d 1069, 1072 (D.S.D. 2001) (extending CDA immunity to copy center that permitted third-party users to send e-mails and other electronic communications anonymously).

170. Does 1 Through 30 Inclusive v. Franco Prods., 99 C 7885, 2000 U.S. Dist. LEXIS 8645, at *10–16 (N.D. Ill. June 22, 2000), *aff'd sub nom.* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

171. Doe v. America Online, Inc., 783 So. 2d 1010, 1013–17 (Fla. 2001) (dismissing case filed by parent of young boy seduced after being contacted by pedophile in AOL chat room); Jane Doe One v. Oliver, 755 A.2d 1000, 1003–04 (Conn. Super. Ct. 2000) (holding AOL immune from improper e-mail messages sent to plaintiff mother's employer), *aff'd*, 792 A.2d 911 (Conn. App. Ct. 2002).

172. Schneider v. Amazon.com, Inc., 108 Wash. App. 454, 458, 467, 31 P.3d 37, 39, 43 (2001).

173. *See, e.g., Ben Ezra, Weinstein, & Co.*, 206 F.3d at 984–86 (holding defendant ISP immune from suit pursuant to § 230 because AOL was not "publisher or speaker" of defamatory speech); Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (holding § 230 protects ISP from liability for defamatory speech initiated by third party); Smith v. Intercosmos Media Group, Inc., No. CIV.A.02-1964 sec. C, 2002 U.S. Dist. LEXIS 24251, at *7–12 (E.D. La. Dec. 17, 2002)

infliction of emotional distress,[175] and for spam lawsuits.[176] The courts, however, have steadfastly refused to extend immunity to trademark or copyright infringement occurring on websites.[177]

When interpreting § 230, courts have consistently classified Internet defendants as conduits even when they play an active editorial role.[178] Nearly all courts rule that ISPs are not liable for defamation, even if they perform "traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content."[179] In *Batzel v. Smith*,[180] the

---

(denying relief for defamation, libel, or negligence based on allegedly defamatory websites set up by its customers); *PatentWizard, Inc.*, 163 F. Supp. 2d at 1071–72 (ruling provider was not liable for anonymous Internet user's disparaging remarks about plaintiffs' software in chat room session where plaintiffs were unable to determine identity of user because provider did not record identities of persons who rented its computers); Marczeski v. Law, 122 F. Supp. 2d 315, 326–28 (D. Conn. 2000) (holding individual defendants who created chat room were immunized by § 230); *see also Schneider*, 108 Wash. App. at 467, 31 P.3d at 43 (dismissing defamation lawsuit against Amazon.com for third party's posting of negative comments about author's book on site).

174. Green v. America Online, Inc., 318 F.3d 465, 471 (3d Cir. 2002); *Zeran*, 129 F.3d at 330.

175. Whether a wrong rises to the requisite level of outrageousness and egregiousness to sustain a claim for intentional infliction of emotional distress is a question of law. If the evidence shows that reasonable persons might find the presence of extreme and outrageous conduct and resulting severe emotional distress, a jury then must find the facts and make its own determination. To support the emotional distress allegation, the conduct must have been so abusive or obscene as naturally to humiliate, embarrass, frighten, or extremely outrage a plaintiff. Ramey v. Darkside Prods., Inc., No. CIV.A.02-730 (GK), 2004 U.S. Dist. LEXIS 10107, at *12–18 (D.D.C. May 17, 2004) (granting summary judgment in favor of publisher of online advertising guide for adult entertainment on tort claims of intentional infliction of emotional distress, unjust enrichment, negligence, and fraud).

176. Batzel v. Smith, 333 F.3d 1018, 1034 (9th Cir. 2003) (holding federal statutory immunity available to Internet intermediaries under 47 U.S.C. § 230(c)(1) (2000) applies only when "a reasonable person in the position of the service provider or user would conclude that the information was provided for publication on the Internet or other 'interactive computer service'"); OptInRealBig.com, LLC v. IronPort Sys., Inc., 323 F. Supp. 2d 1037, 1047 (N.D. Cal. 2004) (holding CDA immunizes anti-spam software company from liability).

177. A court rejected a website's contention that it was classified as an interactive computer service provider and thus was protected from liability for the trademark infringement of its customers. Ford Motor Co. v. GreatDomains.com, Inc., 60 U.S.P.Q.2d (BNA) 1446, 1447 (E.D. Mich. 2001). However, as the court noted, § 230 of the CDA expressly provides that "nothing in this section shall be construed to limit or expand any law pertaining to intellectual property." *Id.*; *see* 47 U.S.C. § 230(e)(2).

178. *See, e.g.*, Stoner v. eBay, Inc., No. 305666, 2000 WL 1705637, at *1 (Cal. Super. Ct. Nov. 1, 2000) (classifying online auction website as interactive computer service provider even though site does not enable access to Internet and exercises editorial control and monitoring); *Schneider*, 108 Wash. App. at 465–67, 31 P.3d at 42–43 (extending immunity to online bookstore which posts reviews of books by readers and has searchable database where people locate and purchase books).

179. *Zeran*, 129 F.3d at 330, 331; *see, e.g.*, *Batzel*, 333 F.3d at 1031 (vacating district court order denying website operator's anti-SLAPP motion and remanding to district court for further proceedings to evaluate what provider should have reasonably concluded at time he received e-

court noted that the congressional exclusion of "publisher" liability for third-party content also shields providers for "the usual prerogative of publishers to choose among proffered material and to edit the material published while retaining its basic form and message."[181] Courts have conflated distributors' liability with publishers' liability, blithely ignoring distinctions developed over centuries of tort law.

The courts' expansive interpretation of § 230 has resulted in an inhospitable legal environment for consumers in cyberspace. Some of the injustices caused by § 230 decisions are shocking in the extreme, just like the iniquitous results of the common law rule that there is no duty to aid one in peril.[182] A gold medalist swimmer, for example, "with a boat and a rope at hand, who sees another drowning before his eyes, is not required to do anything at all about it."[183]

Modern courts impose a duty on innocent injurers to assist their victims who have been placed in a position of peril.[184] When a website realizes that its services have created a condition involving an unreasonable risk of a cybertort, it should also have a duty to mitigate damages. Websites are not necessarily mere pipes or conduits; they also play a role in creating or enabling cybertorts or infringement.

Websites can facilitate defamation, pornography, and wholesale invasions of privacy without the risk of tort liability. The harsh effects of nineteenth century no-duty rules were toned down by doctrines such as the duty of common carriers to take reasonable steps to save passengers in peril.[185] Under maritime law, a ship's captain has a duty to save a seaman who has fallen overboard.[186] ISPs are the modern-day functional equivalent of common carriers in cyberspace, and they should have a responsibility to come to the aid of website visitors and customers when

---

mail); Ben Ezra, Weinstein, & Co. v. America Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000) (reasoning "Congress clearly enacted § 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions"); Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998) (interpreting § 230 as immunizing providers for exercise of editorial and self-regulatory functions).

180. 333 F.3d 1018 (9th Cir. 2003).

181. *Id.* at 1031.

182. KEETON ET AL., *supra* note 98, § 56, at 375 (noting that there is no legal duty to come "to the aid of another human being who is in danger, even if the other is in danger of losing his life").

183. *Id.*

184. RESTATEMENT (SECOND) OF TORTS § 321 cmt. a (1965) (noting there is duty whether original act is tortious or innocent).

185. KEETON ET AL., *supra* note 98, § 56, at 376.

186. *Id.*

they have well-defined notice of continuing crimes and torts on their services.

The unintended consequence of immunizing all ISPs from tort liability is that this confers an absolute immunity on feral ISPs that harm the public. In *Ramey v. Darkside Productions, Inc.*,[187] an online adult services website published unauthorized sexually explicit photographs of the plaintiff in its Eros Guide, using content supplied by a customer.[188] The court ruled that the pornographic website was immunized from liability for the plaintiff's tort claims, even though it had actual notice that the photographs infringed the intellectual property rights of the exotic dancer.[189] The *Darkside* court described the § 230(c) "immunity as quite robust, adopting a relatively expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'" [190] The website compartmentalized its adult entertainment content and even placed a watermark on the unauthorized photographs.[191] Despite these compelling facts, the court ruled that the federal immunity for publishers applied, granted summary judgment in favor of the pornographer, and left the plaintiff with no redress for her injuries.[192]

In *OptInRealBig.com, LLC v. IronPort Systems, Inc.*,[193] a spam e-mailer sought a preliminary injunction to enjoin SpamCop.net[194] from publishing reports about alleged spammers and eradicating e-mail addresses of those complaining about spam.[195] The bulk e-mailer alleged that the anti-spam program[196] inflated the complaints against it and

187. 2004 U.S. Dist. LEXIS 10107 (D.D.C. May 17, 2004).

188. *Id.* at *6.

189. *Id.* at *16–18.

190. *Id.* at *20.

191. *Id.* at *5–6.

192. *Id.* at *20.

193. 323 F. Supp. 2d 1037 (N.D. Cal. 2004).

194. The court described SpamCop as:

> an interactive Internet-based service whose mission is to reduce spam by reporting complaints to ISPs that provide Internet access to the senders of spam ("spammers"). Whereas many anti-spam companies provide filtering services, which blocks [sic] an anti-spam customer from receiving spam, SpamCop goes one step further. It forwards complaints to ISPs to encourage ISPs to sanction spammers, including cutting off the spammers [sic] bandwidth (e.g. their access to the Internet). . . . SpamCop's founder, Julian Haight, has stated that he has helped close many spammers' e-mail accounts.

Id. at 1040 (citations omitted).

195. *Id.* at 1038–39.

196. "Plaintiff in this case, OptIn, is in the business of sending bulk commercial e-mails.

caused ISPs to reduce the bandwidth it needed to run its business.[197] OptIn charged that the anti-spam company was intentionally interfering with its contracts,[198] was defaming its business reputation,[199] and constituted unfair competition.[200]

The federal district court ruled that OptIn was not entitled to a preliminary injunction because the spam reduction business is immune from publisher's liability under the CDA, despite the fact that SpamCop exercised many traditional functions of publishers.[201] The court held that the anti-spam company was an ISP that used interactive computer services to distribute its online mailing, post reports from registered users, and send report copies to non-subscribers.[202] The court immunized the defendant, even though it was aggressive in its mailings, because it had not altered the content of the messages it received.[203] While the result in this case benefited consumers by restraining spam, overly broad immunities generally work to the advantage of online pornographers, spam e-mailers, vendors of bogus goods, forged financial services, and pyramid schemers.

Defendant, SpamCop, is in the business of collecting complaints from recipients of alleged spam and forwarding these complaints to Internet Service Providers ('ISPs') who supply Internet bandwidth to the purported spammers." *Id.* at 1039.

197. *Id.*

198. A plaintiff claiming interference with prospective economic advantage must prove:

> (1) the existence of an economic relationship between the plaintiff and a third party; (2) that the defendant was aware of the relationship and acted wrongfully with the purpose of disrupting the relationship; (3) that the relationship was disrupted; and (4) that the plaintiff suffered damages that flow proximately from the disruption. The wrongful act must be conduct that was wrongful by some legal measure other than the fact of interference itself.

Id. at 1049 (citations omitted).

199. To prevail in a claim for trade libel, a plaintiff must demonstrate that the defendant: (1) made a statement that disparages the quality of the plaintiff's product; (2) that the offending statement was couched as fact, not opinion; (3) that the statement was false; (4) that the statement was made with malice; and (5) that the statement resulted in monetary loss. *Id.* at 1048.

200. *Id.* at 1039.

201. The court ruled that SpamCop was immune because it was classified as an interactive computer service. *Id.* at 1051–52. The court noted that, even if the defendant was not immune, it would deny the injunction because the e-mail business was not likely to succeed on the merits of its claims, it was unclear whether the e-mail business's harm emanated from the spam complaint business's acts, and the public interest in protecting privacy and free speech outweighed whatever risks the e-mail business faced. *Id.*

202. *Id.* at 1047.

203. *Id.*

C. *Cybertort Law Is Not Settled Until It Is Settled Right*

In *Zeran v. America Online, Inc.*,[204] the U.S. Court of Appeals for the Fourth Circuit expanded the scope of CDA immunity by ruling that § 230 abolished distributor liability even when the ISP has knowledge of the defamatory content.[205] The World Wide Web would grind to a halt if ISPs were required to monitor all e-mail or Internet communications on their services.[206] An ISP is frequently in the position of being merely a distributor of content to its subscribers. AOL, for example, contracts with content providers to provide its subscribers with special features such as musical concerts, online chats with celebrities, and sporting events. It merely posts content supplied by third parties; it does not monitor the materials. ISPs need some protection against liability, but the current legal regime is tilted too far in their favor.

This imbalance in favor of ISPs is clearly demonstrated in cases like *Zeran v. America Online, Inc.* In *Zeran*, the court affirmed summary judgment in favor of an ISP on the grounds of § 230 immunity in a case in which an impostor posted defamatory messages on the ISP's bulletin board.[207] The sham posting accused the plaintiff, Ken Zeran, of selling offensive t-shirts celebrating the Oklahoma City bombing.[208] Zeran received hundreds of threatening telephone calls, flaming e-mails, and death threats as a result of the phony postings.[209]

AOL did not promptly remove the false listings, refused to retract the sham postings, and did not take steps to block further defamatory postings by the impostor.[210] The *Zeran* court ruled that AOL could not be held liable because it was entitled to immunity as either a publisher or a distributor of defamatory statements posted on its service.[211] The court

---

204. 129 F.3d 327 (4th Cir. 1997).

205. *Id.* at 332.

206. As the *Zeran* court noted:

> The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for 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 service providers might choose to severely restrict the number and type of messages posted.

Id. at 331.

207. *Id.* at 328.

208. *Id.* at 329.

209. *Id.* at 330.

210. *Id.* at 329.

211. *Id.* at 332 (ruling that "AOL is legally considered to be a publisher" and that "[e]ven distributors are considered to be publishers for purposes of defamation law").

found the long-standing common law differentiation between publisher and distributor liability to be a distinction without a difference.[212] The court refused to consider AOL as either a publisher or distributor, despite the ISP's notice of tortious activity on its services: "Assuming *arguendo* that Zeran has satisfied the requirements for imposition of distributor liability, this theory of liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230."[213]

The *Zeran* court feared that, "[i]f 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."[214] The court's concern that imposing distributor liability on ISPs would result in legal overkill is unsupported by any empirical research. During centuries of common law development, the rule of distributor liability has never produced a flood of claims. The vast majority of courts follow *Zeran* in granting broad immunity to providers even when they have an active role in distributing defamatory materials provided by third parties for publication.[215] ISPs also have no liability for third party content, even if they can easily render inoperative those website postings that are known to be illegal.

Courts have granted publisher's immunity to ISPs that were clearly more than mere content distributors. For example, in *Blumenthal v.*

---

212. The court stated:

> The terms "publisher" and "distributor" derive their legal significance from the context of defamation law. . . . Because the publication of a statement is a necessary element in a defamation action, only one who publishes can be subject to this form of tort liability. . . . Publication does not only describe the choice by an author to include certain information. In addition, both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party . . . constitute publication.

Id. (citations omitted).

213. *Id.*

214. *Id.* at 333.

215. *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124–25 (9th Cir. 2003) (extending immunity to online dating service that collected, categorized and organized information provided by third parties); Green v. America Online, Inc., 318 F.3d 465, 471–72 (3d Cir. 2003) (rejecting plaintiff's argument that AOL was divested of its § 230 immunity "because AOL's Community Guidelines outline standards for online speech and conduct and contain promises that AOL would protect [plaintiff] from other subscribers"); Ben Ezra, Weinstein, & Co. v. America Online, Inc., 206 F.3d 980, 985–86 (10th Cir. 2000) (refusing to strip ISP of § 230 immunity in negligence-based lawsuit for inaccurate stock quotations even when provider played editorial role by making editorial deletions and corrections); Blumenthal v. Drudge, 992 F. Supp. 44, 51–53 (D.D.C. 1998) (holding service provider immune from liability even though it paid online political gossip for information and promoted content on its services).

Drudge,[216] the court held that AOL was entitled to immunity despite fulfilling many roles of a primary publisher.[217] AOL was inoculated from defamation liability as a § 230 provider, despite the fact that the ISP had an exclusive contract to electronically publish Matt Drudge's political gossip column on its services.[218]

In this case, White House aide Sidney Blumenthal filed a defamation case against AOL and Matt Drudge after Drudge erroneously reported that Blumenthal had a "spousal abuse past." AOL and Drudge promptly published a retraction of the cybersmear.[219] The court dismissed AOL from the case after classifying the company as an ISP immunized by § 230.[220] The plaintiff charged that AOL was a distributor masquerading as a mere conduit.[221] The court rebuffed that contention, stating that "[a]ny attempt to distinguish between 'publisher' liability and notice-based 'distributor' liability and to argue that Section 230 was only intended to immunize the former would be unavailing."[222] The court concluded that "the statutory language is clear: AOL is immune from suit" as either a publisher or distributor.[223]

The trial judge conceded that it was an injustice to not hold a service provider responsible where it was clearly more like a disguised publisher than a true conduit for third-party content:

> If it were writing on a clean slate, this Court would agree with plaintiffs. AOL has certain editorial rights with respect to the content provided by Drudge and disseminated by AOL, including the right to require changes in content and to remove it; and it has affirmatively promoted Drudge as a new source of unverified instant gossip on AOL. Yet it takes no responsibility for any damage he may cause. AOL is not a passive conduit like the telephone company, a common carrier with no control and therefore no responsibility for what is said over the telephone wires. Because it has the [right] to exercise editorial control over

216. 992 F. Supp. 44 (D.D.C. 1998).

217. Matt Drudge and AOL entered into an exclusive license agreement that "made the Drudge Report available to all members of AOL's service for a period of one year. In exchange, defendant Drudge received a flat monthly 'royalty payment' of $3,000 from AOL." *Id.* at 47.

218. *Id.* at 50.

219. *Id.* at 48.

220. *Id.* at 51.

221. *See id.* at 47, 50.

222. *Id.* at 52.

223. *Id.* at 53.

> those with whom it contracts and whose words it disseminates, it would seem only fair to hold AOL to the liability standards applied to a publisher or, at least, like a book store owner or library, to the liability standards applied to a distributor.[224]

Individual plaintiffs will not have realistic cybertort remedies until the scope of § 230 of the CDA is scaled back to Congress's original intent of insulating providers from claims for publisher's liability arising out of third-party content.

D. A Possible New Path for Cybertort Law

This is a propitious moment to revisit the matter of ISP tort liability. The California Court of Appeal recently noted that most scholars believe that the expansive reading of § 230 "is flawed in that the court ascribed to Congress an intent to create a far broader immunity than that body actually had in mind or is necessary to achieve its purposes."[225] The Supreme Court of California has granted a petition for review to consider the reach of § 230 in a case where the ISP was more than a passive conduit, engaging in many traditional editorial functions though falling short of being the primary content creator.[226]

In *Barrett v. Rosenthal*,[227] a California court of appeal became the first U.S. court to hold that § 230 does not immunize an ISP that republishes defamatory statements authored by a third party after the website acquires knowledge that the statements were false.[228] The appeal court's milestone decision adopted the common law rule that distributors are liable for transferring defamatory information if they have

---

224. *Id.* at 51–52.

225. Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 154 (Cal. Ct. App. 2004) (citations omitted), *review granted and opinion superseded by* 87 P.3d 797 (Cal. 2004).

226. The court stated:

> In addition to the issues set forth in the petition for review, the court requests the parties to include briefing on the following questions: (1) What is the meaning of the term "user" under section 230 of the Communications Decency Act (47 U.S.C. section 230)? (2) For purposes of the issue presented by this case, does it matter whether a user engaged in active or passive conduct?

Barrett v. Rosenthal, 87 P.3d 797, 797 (Cal. 2004) (order granting review).

227. 9 Cal. Rptr. 3d 142 (Cal. Ct. App. 2004), *review granted and opinion superseded by* 87 P.3d 797 (Cal. 2004).

228. *Id.* at 154. "Since the decision in *Zeran*, no court has subjected a provider or user of an interactive computer service to notice liability for disseminating third-party defamatory statements over the Internet, though a three-judge minority of the Florida Supreme Court would have done so." *Id.* at 153.

knowledge of its objectionable content.[229] The Supreme Court of California granted a petition for review after the court of appeal vacated in part and otherwise affirmed an order granting a special motion to strike.[230]

In *Barrett*, plaintiffs Stephen Barrett and Terry Polevoy, two medical doctors, were "primarily engaged in combating the promotion and use of 'alternative' or 'nonstandard' healthcare practices and products."[231] The physicians maintained Internet "[w]eb sites that expos[ed] 'health frauds and quackery' and provid[ed]" consumers with information about health care alternatives.[232] One defendant, Rosenthal, was an alternative health practitioner who reprinted and distributed a number of bogus charges against the plaintiff physicians.[233]

The defendant's web postings charged the two doctors with running a "Slea[z]y 'Quack buster' Scam,"[234] and charged that Dr. Polevoy stalked women.[235] Rosenthal refused to withdraw the antagonistic postings and posted thirty-two additional messages on Internet newsgroups denouncing the doctors' threatened litigation.[236] These messages included a copy of the original allegedly defamatory message or a reference back to that message and referred to the doctors as, among other things, "quacks."[237]

After the defendant rebuffed requests to remove the denigrating messages, the plaintiffs filed suit for libel, conspiracy, and libel per se.[238] The trial court dismissed their complaint because it contravened California's anti-SLAPP (Strategic Lawsuits Against Public Participation) statute, which protects a defendant's right of free speech if a plaintiff's cause of action arises from protected activity.[239] The court found inadequate evidence that the defendant's defamatory statements

229. *Id.* at 152 (holding that CDA does not "abrogate the common law principle that one who republishes defamatory matter originated by a third person is subject to liability *if he or she knows or has reason to know of its defamatory character*") (citing RESTATEMENT (SECOND) OF TORTS § 581(1)) (emphasis in original).

230. *Barrett*, 87 P.3d at 797; *Barrett*, 9 Cal. Rptr. 3d at 167.

231. *Barrett*, 9 Cal. Rptr. 3d at 144.

232. *Id.*

233. *Id.* at 144–45.

234. *Id.* at 146.

235. *Id.* at 145.

236. *Id.* at 146.

237. *Id.*

238. *Id.* at 145–46.

239. *Id.* at 146.

had harmed the plaintiffs' reputational interests.[240]

The California Court of Appeal affirmed the application of the anti-SLAPP statute as to Dr. Barrett, but not as to Dr. Polevoy.[241] The court found that the trial court went astray in requiring Dr. Polevoy to demonstrate actual damages because the defamatory language posted on the website was libel per se.[242] The court held that the federal immunity granted by § 230 was inapt because Rosenthal was a "user of an interactive computer service" and a primary publisher who was strictly liable for defamatory statements.[243] The court ruled that § 230 does not "abrogate the common law principle that one who republishes defamatory matter originated by a third person is subject to [distributor] liability *if he or she knows or has reason to know of its defamatory character*."[244]

The *Barrett* appellate court flatly declined to follow the *Zeran* court's reasoning that § 230 "immunized providers and users of interactive computer services from liability not only as primary publishers but also as distributors."[245] The *Barrett* court noted that § 230, on its face, does not clearly address whether Congress intended to overthrow the well-established common law principle of distributor liability.[246] The court found no evidence that Congress intended § 230 immunity to extend to distributors with knowledge.[247] The *Barrett* court held that providers or users who knowingly distribute defamatory materials produced by third parties should be subject to liability.[248]

If the Supreme Court of California affirms the appellate court, it will further demonstrate that "the common law [is] at its best in accommodating change within the framework of continuity."[249] This case may well be a bellwether decision that will reshape online intermediary law. The court may conclude that Congress intended § 230

240. *Id.*

241. *Id.*

242. *Id.* at 146–47.

243. *Id.* at 151–52.

244. *Id.* at 152 (emphasis in original) (citing RESTATEMENT (SECOND) OF TORTS § 581(1) (1977)).

245. *Id.* at 153 (emphasis omitted).

246. *Id.* at 155–56.

247. *Id.* at 156.

248. *Id.* at 160–61.

249. Thomas F. Lambert, Jr., *Tort Liability for Psychic Injuries: Overview and Update*, 37 ATLA L.J. 1, 27 (1978).

to encompass absolute immunity for third party communications as either publishers or distributors, even if the ISP is engaged in active conduct such as editing, screening, or commissioning content. The trend of online intermediary law points in this direction. Alternatively, the court could construe § 230 to immunize an ISP as a publisher but not a distributor, which is consistent with the CDA's statutory language.

A decision by the Supreme Court of California that downsizes § 230 would open the door to a greatly needed radical reconsideration of the duty of care in cyberspace. Interactive computer services should not be absolved of all responsibility when they have actual knowledge of defamatory postings or e-mails. Similarly, when a website operator has knowledge that a posting overruns the privacy or tarnishes the reputation of a computer user, it should have a duty to retract the deprecating publication or prevent further tortious or criminal activity.

Imposing limited liability is only the first step toward making ISPs more accountable to the public for excessive preventable dangers in cyberspace. When losses are placed on the online intermediaries, the total price tag to society is lowered. For example, an ISP is in the preeminent position to publish cost-efficient retractions of defamatory communications that will result in more truthful information being provided to the public. In the case of an Internet trade libel, an ISP's prompt action will decrease the radius of the financial injury and lessen losses from trade libel such as plummeting stock market values. Limited liability will induce ISPs to expand system-wide products to protect all users from viruses, spyware, spam, and security holes. Online intermediaries are in the best position to calibrate Internet security to the radius of the risk and in proportion to the peril because they are generally the first to detect the problem.

Once ISP immunity is reduced, it is likely that courts will begin to impose a duty of care on online information providers to act sensibly in protecting their customers from third-party crimes and torts. Requiring ISPs to take down abhorrent materials, such as the secret videotapes of the college athletes, will steadily grind down the liability-free zone that these entities currently enjoy. The overall rate of tort injuries to consumers will be diminished if ISPs have an inducement to implement security solutions to detect and thwart cybercriminals. For example, the computer industry has already developed systems of deception, such as decoys, "fly traps," and "honeypots," in order to trap unwary computer

intruders.[250] The imposition of a greater duty of care will rekindle research into how to plug security holes, trap cybercriminals, block spam, disable pornographic pop-ups, and stifle the growth of website creepy crawlers.

III. THE INJURY PROBLEM FOR "ONE-SHOTTERS" IN CYBERSPACE

Our statistical analysis clearly demonstrates that online consumers and many other victims of cyberspace harms have been unable to obtain redress through traditional tort law. Consumer actions against online sellers and service providers are simply missing from the litigation landscape. The lack of consumer victories can largely be explained by the problem of locating the primary wrongdoer and, as shown in Part II, the immunity enjoyed by most Internet sellers.

This Part develops the case for creating stronger remedies for consumers and other computer users to redress online injuries. The World Wide Web provides a cross-national instrumentality for online defamation, intentional infliction of emotional distress, fraud, and other Internet-related wrongdoing that is unlikely to be punished. The misuse of the Internet has created a "tragedy of the anti-commons."[251] Without effective enforcement of consumer rights and remedies, the Internet will not fulfill its promise as a secure marketplace for procuring goods or services.

A. ISPs Have No Duty to Cooperate with Injured Consumers

This blanket ISP immunity for hosting or posting the content provided by third parties has resulted in numerous injustices. Not only are ISPs immune from lawsuits for hosting or posting third party content, but also they have no legal duty to cooperate with the plaintiff in tracking down cybercriminals. The absolute immunity given to web hosts and other providers makes it all but impossible for plaintiffs to learn more about the role of ISPs in creating, developing, or designing websites or web pages where tortious activities are taking place.

In *Doe v. GTE Corp.*,[252] for example, three different corporations

250. ISP Planet, *Intrusion Detection Services Directory*, *at* http://isp-planet.com/services/ids (last visited Mar. 12, 2005).

251. Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 442 (2003).

252. 347 F.3d 655 (7th Cir. 2003).

provided Internet access and web hosting services for Franco Productions, a pornographer that sold unauthorized tapes of college athletes filmed secretly while they were showering or dressing.[253] The victims learned of the existence of films such as *Voyeur Time* and *Between the Lockers* from a newspaper story about the adult services website.[254] The federal court of appeals ruled that the college athletes had no cause of action against the ISPs that had profited from hosting the adult services websites.[255] The imposition of distributor liability would give these athletes and the many other victims of online misconduct a right to have illegal or objectionable material removed.

The plaintiffs were not even able to obtain discovery to determine how extensively GTE and the other web hosts participated in "designing or creating or maintaining the web site, ranging anywhere from completely creating, writing, organizing and originally editing content before it is posted and changing, updating, adding or deleting content thereafter, to providing the template or architecture of the web site."[256] At present, courts typically will dismiss service providers from tort actions filed against them early in the litigation, prior to discovery. In many cybertort cases involving a third-party criminal, a plaintiff will be unable to use discovery to uncover what the service provider knew about prior similar incidents or whether it had a contract or other close connection to the anonymous defendant.[257]

Discovery generally cannot be deployed to establish whether a website operator or service provider aided or abetted a third-party

253. The federal district court described the case as involving

> intercollegiate athletes who, without their knowledge or consent, were videotaped in various states of undress by hidden cameras in restrooms, locker rooms, or showers. The resulting videotapes were sold by various means, including web sites hosted by Genuity.net and TIAC.Net that included still images of the [p]laintiffs taken from the videotapes.

Does 1 Through 30 Inclusive v. Franco Prods., No. 99 C 7885, 2000 U.S. Dist. LEXIS 8645, at *2 (N.D. Ill. June 22, 2000), *aff'd sub nom.* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

254. *GTE Corp.*, 347 F.3d at 656.

255. The district court dismissed all claims against the providers, citing 47 U.S.C. § 230(c) (2000). *GTE Corp.*, 347 F.3d at 657–62. "After the judgment became final with the resolution or dismissal of all claims against all other defendants—the defaulting defendants were ordered to pay more than $500 million." *Id.* at 656–57 (citing *Franco Prods.*, 2002 U.S. Dist. LEXIS 24032, at *2–3). The $500 million judgment is uncollectable because the adult services defendants vanished. *Id.* at 657.

256. *Franco Prods.*, 2000 U.S. Dist. LEXIS 8645, at *7.

257. Microsoft, for example, made a corporate decision to shut down its chat rooms after learning that these sites were notorious venues for the stalking of children by pedophiles. Charles Arthur, *Microsoft Closes Chat Rooms to Curb Pedophile Threat*, INDEPENDENT (London), Sept. 23, 2003, at 1 (reporting closure of United Kingdom chat rooms used by 1.2 million visitors per month).

cybercriminal or tortfeasor who used its services to sell illegal content.[258] For example, the U.S. Court of Appeals for the Tenth Circuit, in *Ben Ezra, Weinstein, & Co., Inc. v. America Online, Inc.*,[259] affirmed a federal magistrate's order denying discovery on the grounds of § 230 immunity.[260] In *Ben Ezra*, the magistrate judge ruled that the plaintiff did not sufficiently respond to the service provider's summary judgment motion and thus had failed to demonstrate why further discovery should be allowed.[261] Early dismissal from these cases means that a plaintiff will typically be unable to learn whether the service provider was connected closely enough to the third party to be unclothed of its immunity.

If § 230 immunity were limited to protection from publisher's liability, a wronged consumer could obtain further discovery in cases where a service provider had actual knowledge of ongoing crimes or torts. Prolonged discovery in cases where the ISP is classified as a distributor will enable plaintiffs to uncover more information about the nature, nexus, and extent of prior crimes and torts on websites. Plaintiffs could use the locomotive of discovery to unearth aggravating factors, such as whether the ISP profited by being too closely connected to fraudulent schemes that injured consumers. Discovery in these cases might even result in ISPs or websites being stripped of their immunity as primary publishers because of a close connection to the creators of illegal content. If ISPs were liable as distributors with knowledge, the gravamen of a case would shift to determining how much the web host or service provider knew about the dishonest scheme and when they knew it.

B. ISPs Are in the Best Position to Prevent Cybertort Injuries

This expansive immunity is a great source of inefficiency in the U.S.

---

258. In *John Does 1 Through 30 Inclusive v. Franco Productions*, 2000 U.S. Dist. LEXIS 8645, (N.D. Ill. June 22, 2000), *aff'd sub nom.* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003), the plaintiffs argued that without further discovery about the creation and development of the website, they could not determine the role of the web host in the sale of secret tapes of college athletes in various stages of undress. *Id.* at *7–8. The plaintiffs request for discovery was rejected because the court dismissed this defendant from the lawsuit. *Id.* at *16, *19.

259. 206 F.3d 980 (10th Cir. 2002).

260. *Id.* at 984 (holding that because it was undisputed that AOL fit within § 230's definition of interactive computer service, it was not abuse of discretion for magistrate to deny further discovery against provider).

261. *Id.*

legal system because ISPs are normally in the preeminent position to deter cyberstalking and other blameworthy activities of their Internet customers. An ISP, for example, will have a log of Internet activity that is a valuable resource for tracking down primary wrongdoers. If an ISP had a legal responsibility to remove defamatory postings, it could easily mitigate damages by terminating the cybercriminal's account, and auditing his illegal activities; this would eliminate ongoing patterns of fraud, such as those in the Yahoo! automobile sales website.

ISPs and websites should have a duty to disable sites where they have actual notice of ongoing deceitful sales and services. Just as a telephone company has records of calls or other subscriber information, an ISP is typically in the best position to keep logs, subscriber information, and software audits of anomalies. A service provider is typically the first to learn of network intrusions or spoofing because it monitors packets traversing its system. An ISP also will be the first to discover attempted break-ins by cybercriminals and can use port scans to mitigate the damage caused by intrusions.

C. *Limiting ISP Immunity Would Help Solve the Injury Problem*

Our synoptic sketch of ISP defamation cases demonstrates the need to limit the CDA's unconditional immunity for third-party postings. If the common law "distributor with knowledge rule" were extended to cyberspace, AOL would be liable for not taking prompt remedial actions in both the *Zeran* and *Blumenthal v. Drudge* cases. Zeran would have an action against AOL for failing to take down the defamatory materials or blocking the reposting of material known to be objectionable. In addition, there would be liability for failing to publish a retraction to repair Zeran's reputation. In the *Blumenthal* case, the plaintiff would be permitted to conduct further discovery about AOL's editorial role in its electronic publication of the Drudge Report. If AOL played a major role in the cooperative creation of content, it would be stripped of its immunity. AOL would have constructive knowledge that Drudge's posting was defamatory and would be held liable as a distributor under the "constructive notice" doctrine of the common law of defamation.[262]

262. The distributor with notice rule would make a telegraph company, for example, liable as a secondary publisher or distributor "if, but only if, it knew or had reason to know that the sender was not privileged to send the message." KEETON ET AL., *supra* note 98, § 113, at 811. There is a distinction between constructive and actual knowledge of defamatory content. If the constructive or actual notice rule applied to AOL, it would likely be liable for Drudge's communication. When it contracted with Drudge to exclusively publish his column online, AOL had constructive knowledge

It is difficult to believe that, when it enacted § 230, Congress meant to grant an unqualified safe harbor for websites that are closely connected to fraudulent schemes or illegal content. The *Zeran* court's interpretation of the CDA not only "mischaracterizes the defamation common law, but it also assumes that Congress had the same oversight."[263] AOL clearly would have been liable as a distributor if the court had accurately construed the statutory language of § 230 because Congress never mentions distributors. AOL should have been held liable under the common law because it had either constructive or actual knowledge of Drudge's defamatory content.

These cases document the rationale for limiting ISP immunity by imposing the distributor with notice rule.[264] This Article proposes that service providers be held responsible for minimizing injuries sustained by their customers so that ISPs have an incentive to increase Internet security.[265] This modest tort reform will help to put cybertort law in motion by requiring that an ISP take on a more dynamic role in preventing ongoing torts in cyberspace. Overly broad immunities have historically encouraged corporate irresponsibility and this pattern continues to this very day.[266]

---

that it was a political gossip column. The ISP may not have had actual knowledge that Drudge's content was defamatory, but it is arguable that AOL should be stripped of its immunity as a publisher because of its editorial role in shaping the content and website. Further discovery would be required to know whether AOL had actual knowledge about Drudge's derogatory communications about Blumenthal.

263. Sewali K. Patel, Note, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 682 (2002).

264. This is also the approach adopted by the intermediate court in *Barrett v. Rosenthal*, 5 Cal. Rptr. 3d 416, 436–38 (Cal. Ct. App. 2003) (holding that § 230 did not abrogate common law principle that one who republished defamatory matter originated by third person was subject to liability if he or she knew or had reason to know of its defamatory character), *vacated on other grounds by* 9 Cal. Rptr. 3d 142 (Cal. Ct. App. 2004).

265. ISP Planet, *supra* note 250 (explaining that ISP is frequently in best position to detect unauthorized changes to maximize security).

266. After World War II, jurisdiction after jurisdiction abrogated the draconian spousal immunity because it led to frequent injustices. Maryland, for example, abolished interspousal immunity in a case where a husband participated in the gunpoint gang-rape of his wife. Lusby v. Lusby, 390 A.2d 77, 77–78, 88–89 (Md. 1978); *see also* Self v. Self, 376 P.2d 65, 65, 70 (Cal. 1962) (abolishing spousal immunity in case where husband broke wife's arm in assault and battery); Small v. Rockfeld, 330 A.2d 335, 336–37, 344–45 (N.J. 1974) (holding that neither interspousal, nor parent-child immunity barred grandmother's action against her son-in-law for reckless misconduct leading to death of her daughter, defendant's wife). During that same period, there was a movement in the states to abolish governmental immunity. *See, e.g.*, Hargrove v. Town of Cocoa Beach, 96 So. 2d 130, 131, 133 (Fla. 1957) (en banc) (holding city liable for wrongful death of plaintiff unattended by police in jail cell); Jones v. State Highway Comm'n, 557 S.W.2d 225, 226–27 (Mo. 1977) (en banc)

IV. REFORMING ONLINE INTERMEDIARY LAW

As documented in Part I, the field of cybertorts has yet to recognize remedies for negligence-based or strict liability actions. Trial lawyers have organized nearly seventy litigation groups to share knowledge and discovery in particular substantive areas such as workplace injury, tobacco, domestic violence, and artificial heart valves.[267] To date, no litigation group has been organized that specializes in any category of Internet injury.[268] As Part II showed, cybertort litigation has been stillborn because the overly inclusive federal immunity makes it highly implausible that a judgment may be obtained against a solvent defendant.

In this Part, we argue that Congress should amend § 230 to reimpose a regime modeled on the common law's "distributor with knowledge" principle.[269] Absolute immunity made sense in the formative era of the Internet when potential liability might have swamped America Online and other nascent ISPs. As the Internet has matured, a worldwide trend towards imposing greater liability on ISPs is gaining momentum.[270]

(abolishing sovereign immunity of state as well as subordinate governmental units); Ayala v. Philadelphia Bd. of Pub. Educ., 305 A.2d 877, 878 (Pa. 1973) (abolishing governmental immunity against local governmental units).

267. Association of Trial Lawyers of America, *ATLA Litigation Group Policies and Procedures* [hereinafter ATLA], *at* http://atla.org/members/litintro.aspx#1 (last visited Mar. 12, 2005).

268. It is surprising that trial lawyers have not filed suit against service providers who negligently enable the loss of third-party data, fail to prevent computer intrusions, or spread computer viruses by not having up-to-date anti-virus programs.

> Several factors make ISPs attractive defendants in defamation claims, many of which relate to the costs associated with litigation. For example, the author of a defamatory statement will often reside outside the jurisdiction of the plaintiff, whereas the ISP that carried the statement does business in the plaintiff's jurisdiction. It might be difficult, time-consuming, or even impossible, to determine the actual author of the message. And even if the author can be identified, he or she may be judgement proof, whereas the ISP likely has "deeper pockets."

Michael Deturbide, *Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses*, J. INFO. L. & TECH., pt. 1 (Issue Three) (2000) (citations omitted), *available at* http://elj.warwick.ac.uk/jilt/00-3/deturbide.html.

269. Most legal commentators agree that § 230 immunizes intermediaries for publisher's liability but not for distributor liability. Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 637–42 (2001) (arguing that courts have misinterpreted § 230 and should leave distributor liability intact); David R. Sheridan, Zeran v. AOL *and the Effect of Section 230 of the Communications Decency Act upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 167–72 (1997) (stating that when "Congress said 'publisher,' it meant 'publisher,' and not 'distributor'").

270. Martin J. Hayes, *Internet Service Provider Liability: Overview of Internet Service Providers Liability*, *at* http://www.jisclegal.ac.uk/ispliability/ispliability.htm (last visited Apr. 24, 2005).

Under the distributor with knowledge rule, ISPs would have an incentive to widen new technologies for detecting and constraining wrongdoers.

Our reform proposal continues to give ISPs immunity for mere conduit, caching, and hosting activities, unless they have actual notice.[271] We favor a synchronized "notice, takedown, and put-back" regime for all civil and criminal wrongdoing. The ISP with actual notice will be liable for information torts as well as the infringement of intellectual property rights when it does not take prompt corrective measures. Finally, the ISP must act "expeditiously" to remove or disable access to the allegedly infringing material or the subject of the infringing activity.[272]

This Article proposes a rule based on actual knowledge because a *constructive* notice rule creates the danger that ISPs will be overwhelmed with frivolous takedown requests. The constructive knowledge rule assumes that a reasonable ISP should have known about objectionable content and in effect, dictates the monitoring of all content on its services. This inflexible standard would have a chilling effect on free expression by causing some ISPs to shut down their services and by increasing the cost of Internet communications. It would be simply too burdensome to require online intermediaries to scrutinize all of the listservs, websites, or electronic bulletin boards[273] that they host.[274] Imposing too much liability on ISPs will:

---

271. *See* 17 U.S.C. § 512 (2000) (conditioning conduit liability on ISP not modifying or assuming role of content creator and noting that ISP must appoint agent to receive complaints of alleged infringement).

272. *See id.*

273. A bulletin board, in the Internet context, is "a computer-based system giving users access from remote terminals to text and programs contributed by one another and stored centrally." Batzel v. Smith, 333 F.3d 1018, 1027 n.9 (9th Cir. 2003) (quoting OXFORD ENGLISH DICTIONARY 642 (2d ed. 1989)).

274. The Fourth Circuit, in *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), explained the congressional purpose behind § 230 of the CDA:

> 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. 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 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 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 service providers to avoid any such restrictive effect.

Id. at 330–31 (citations omitted).

> encourage the virtually automatic and unthinking removal by intermediaries of material from the public domain. A legal system that not only permits but also encourages on-line intermediaries to indiscriminately eliminate any material from the Internet upon receipt of virtually any notice from third parties will threaten freedom of expression and fair competition.[275]

The imposition of a notice and takedown regime founded upon actual knowledge rather than on mere constructive knowledge strikes a suitable balance between the First Amendment and cybertort liability.

Reforming online intermediary law is a way to jumpstart tort law so that it will evolve to redress online injuries.[276] One of the reasons that cybertorts have not yet developed in the fields of negligence and strict liability is the perception of trial lawyers that ISPs are not worth pursuing because they function in a "liability-free" zone.[277] If ISPs are held liable for failing to take reasonable actions to take down offensive content, trial lawyers will begin to think more creatively to develop other theories of cyberspace liability. Tort law historically has witnessed the elimination of overly broad immunities,[278] allowing Americans to protect our institutions, our bodily integrity, and our right to enjoy property.[279]

A. The Least Cost Avoider in Cyberspace

The ISP is typically in the position of the "least cost avoider" to prevent further harm to Internet users.[280] Professors Ronald Mann and

---

275. ESPRIT PROJECT 27028: Electronic Commerce Legal Issues Platform, *Recommendations to the Commission: Liability for Online Intermediaries*, at 4 (Feb. 9, 2000) [hereinafter ESPRIT Project 27028], *available at* http://europa.eu.int/ISPO/legal/en/lab/991216/recomm_liability.pdf.

276. *See* Anthony J. Sebok, *The Invisible Borderlines of Tort on the Internet*, *in* SELECTED LEGAL ISSUES OF E-COMMERCE 57, 77 (Toshiyuki Kono et al. eds., 2002).

277. To date, the leading trial lawyers' organization has yet to establish any significant litigation groups in Internet-related torts, so presumably the costs must exceed the potential payouts. Litigation groups form to share information to reduce the cost of discovery and to increase efficiencies in the conduct of litigation. ATLA, *supra* note 267.

278. Michael L. Rustad & Thomas H. Koenig, *Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory*, 68 BROOK. L. REV. 1, 38–39 (2002) (surveying erosion of immunities in tort law).

279. *See generally id.* (tracing historical expansion and contraction of American tort rights and remedies).

280. Guido Calabresi developed the concept of the "least cost avoider." *See generally* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL & ECONOMIC ANALYSIS (1970). "In tort law, this consideration answers questions such as who, between two parties, ought to bear liability if there is an accident; and how should that liability be apportioned, if at all?" Robert P. Merges, *As Many as*

Jane Winn note that, "in many contexts . . . an ISP is in a position to hinder wrongful conduct by those whose transmissions pass through its network." [281] They cite the example of the ISP's capability of implementing filters against unsolicited bulk e-mail at a reasonable cost.[282] Broadly speaking, the most economical cost-avoider criterion "corresponds to notions of common-sense causation and responsibility."[283]

The ISP is in a superior position to install software that "yields the greatest net saving (or smallest net loss) in total costs (accident costs plus accident avoidance costs)."[284] Online intermediaries such as AOL are recurrently the only entities that have the available technologies to unveil abusive posters, promptly take down offensive websites, or rescind the accounts of cyber-recidivists. ISPs are in the position of first responder when a consumer is defrauded or suffers other losses as the result of a website swindle. These entities are generally the first to identify unauthorized changes to computer systems that point toward a computer intrusion. For these reasons, online intermediaries should be subject to tort liability where they have actual knowledge of torts or crimes being committed on their services.

The ISP is generally in the best position to develop comprehensive authentication systems to reduce anonymous crimes and torts in cyberspace. In our example of the fraudulent sale of Porsches,[285] Yahoo! is the foremost line of defense against cybertort injuries because it is in the position to receive and evaluate system-wide complaints about sellers who use its services. Yahoo! is the least cost avoider because it maintains audit trails that are likely to expose the architect of an online fraud. However, absent a change in ISP law, Yahoo! has no responsibility to lend a hand to consumers who are victimized by online frauds even if the ISP can readily uncover the wrongdoer's contact information.[286]

Six Impossible Patents Before Breakfast: Property Rights for Business Concepts and Patent System Reform, 14 BERKELEY TECH. L.J. 577, 600 (1999).

281. MANN & WINN, *supra* note 9, at 189.

282. *See id.*

283. Stephen G. Gilles, *Negligence, Strict Liability, and the Cheapest Cost-Avoider*, 78 VA. L. REV. 1291, 1374 (1992).

284. *Id.* at 1316.

285. *See infra* notes 4–6 and accompanying text.

286. Even though the Authors and the seller had an extensive e-mail exchange, we had no way of identifying who the fraudulent seller was or in what country he was located. Yahoo! has no

B. *Adapting European Takedown Regimes*

Our proposed "notice and take-down" reform will bring U.S. tort law into alignment with the European Union community's[287] E-Commerce Directive.[288] The Directive's "notice, take-down and put-back" regime[289] strikes the correct balance between liability and immunity by making the least cost avoider accountable.[290] The E-Commerce Directive requires member states to acknowledge electronic contracts,[291] establishes the liability of Internet intermediaries,[292] provides for online dispute resolution,[293] and harmonizes e-commerce rules.[294] The European Union's Directive "seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States."[295] This legal regime institutes ISP liability rules not only for torts but also for all types of illegitimate activities in cyberspace. The Directive treats all liability horizontally so that it applies "to all kinds of illegal material provided by third parties, including copyright, trademark, defamatory statements, pornography,

---

procedures for assisting consumers in locating wrongdoers and, under current law, has no obligation to assist the defrauded Internet user.

287. *See* Europa, *E-Commerce: EU Law Boosting Emerging Sector*, *at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/03/1580&format=HTML&aged=1&language=EN&guiLanguage=en (last visited Mar. 13, 2005).

288. *See generally* E-Commerce Directive, *supra* note 27.

289. Rosa Julià-Barceló & Kamiel J. Koelman, *Intermediary Liability in the E-Commerce Directive: So Far So Good, But It's Not Enough* (2000) (using this phrase to describe E-Commerce Directive's ISP liability rules), *available at* http://www.ivir.nl/publications/koelman/notenough.html (last visited Mar. 16, 2005). "It must also be kept in mind that the Directive only provides for a system of liability exemptions for ISPs. Thus, if an ISP does not qualify for an exemption under the Directive, its liability will be determined by the national laws of the respective Member States." Baistrocchi, *supra* note 22, at 119.

290. A United Kingdom governmental department noted:

> There is a careful balance to be maintained between, on the one hand, protecting the interests of originators and users of Internet content and, on the other hand, encouraging new intermediaries (especially ISPs) to enter the market (and existing ones to continue). In striking this balance, the Directive seeks to stimulate cooperation between different parties and so reduce the risk of illegal activity online while ensuring that liability can be correctly apportioned.

Department of Trade & Industry, *Industries and Sectors eCommunications: Policy Background*, *at* http://www.dti.gov.uk/industries/content/chapter_6.html (last visited Mar. 13, 2005).

291. E-Commerce Directive, *supra* note 27, at art. 9, at 11–12.

292. *Id.* at art. 12–15, at 12–13.

293. *Id.* at art. 17, at 14.

294. *See generally id.*

295. *Id.* at art. 1, at 8.

etc. Second, as regards the types of liability covered by the Directive, it should be noted that the liability limitations apply not only to civil but also to criminal liability."[296]

Articles 10 through 21 of the E-Commerce Directive "set forth the liability limitations for intermediary service providers and applicable take-down and put-back regimes for illegal material distributed through their facilities."[297] European ISPs are immunized for caching,[298] hosting,[299] and perfunctory tasks related to efficient transmission of digital data. The E-Commerce Directive does not impose liability on the ISP if it does not modify information transmitted by third parties, unless the ISP acquires actual or constructive notice of illegal content and fails to take prompt remedial steps.[300] Article 15(1) makes it clear that Member States may not impose a duty on providers to investigate questionable e-mails or website posters.[301] Article 15(2), however, permits Member States to enact legislation requiring providers to notify law enforcement when they discover illegal activities on their services.[302] One of the complexities of the E-Commerce Directive's constructive notice provision is its insufficient guidance as to what circumstances and requirements place ISPs on notice.[303]

The E-Commerce Directive provides the floorboards but not the

296. Julià-Barceló & Koelman, *supra* note 289.

297. MORRISON & FOERSTER LLP, THE EMERGING EUROPEAN REGIME ON ISP LIABILITY: MEMBER STATES MAKE PROGRESS IMPLEMENTING E-COMMERCE DIRECTIVE (2002), *available at* http://www.softic.or.jp/symposium/open_materials/10th/en/vinje2-en.pdf.

298. E-Commerce Directive, *supra* note 27, at art. 13, at 13.

299. *Id.* at art. 14, at 13.

300. "The directive covers all forms of IP, including copyright, patent and trademark, but would permit member states to go beyond it by enacting greater protections for rights holders in business tort cases and licensing disputes." *U.S., European Groups Coalesce to Combat Controversial Proposal*, 4 WARREN'S WASH. INTERNET DAILY 1 (Aug. 8, 2003) [hereinafter *Controversial Proposal*]. The E-Commerce Directive does not really spell out ISP liability, nor does it provide a methodology for determining damages for contributory infringement. In general, the Directive has been criticized for its vague standards for implementing its takedown regime. Julià-Barceló & Koelman, *supra* note 289.

301. E-Commerce Directive, *supra* note 27, at art. 15(1), at 13.

302. Article 15(2) states:

> Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Id. at art. 15(2), at 13.

303. *See* Julià-Barceló & Koelman, *supra* note 289.

ceiling tiles of protection accorded to European citizens.[304] Member States have the discretion to implement even more rigorous obligations for online intermediaries than the Directive dictates.[305] France, for example, requires ISPs to offer sufficient screening to permit parents to control their children's access to objectionable materials.[306] Each European Member State has the discretion to develop its own procedures to sanction those who violate the Directive.[307]

The benefits of imposing this limited liability come at a price. The current absolute immunity enjoyed by American ISPs has the virtue of drawing a clear line that eliminates any exposure to liability for third-party content. The imposition of even a limited duty for ISPs creates legal uncertainties and new financial burdens. ISPs, for example, need to bear the expenditures of investigating complaints, tracking down wrongdoers, and making nuanced takedown and put-back decisions under European law. These higher costs are passed on to computer users and other consumers in Internet access charges.

The European Union's E-Commerce Directive has also been criticized for promoting self-censorship, the loss of privacy, and a decline in the free flow of information.[308] A Dutch civil rights group did an experiment in which they posted an 1871 document by a well-known Dutch author, which was clearly not protected by copyright, to accounts with ten different ISPs. They next e-mailed bogus takedown notices to each ISP, claiming that they were the valid copyright holder of the document and demanding that it be taken down. Seven of the ten ISPs removed the "objectionable" material, sometimes within hours and without informing

304. One of the major problems with the Directive, unlike the DMCA, is that it is standards-based rather than rule-based. The Directive sets a baseline of protection but leaves it up to the Member States to provide specific protection for "notice and take-down procedures." Another possibility is that the Directive contemplates that industry standards will emerge to supplement, but not supplant the Council's basic principles. *See* Julià-Barceló & Koelman, *supra* note 289.

305. Telephone Interview with Sandra Paulsson, Trainee, Policy Department for Economics and Science, DG2, European Parliament (Nov. 8, 2004).

306. *Id.*

307. *Id.*

308. Two commentators describe how the E-Commerce Directive's takedown procedure clashes with free expression, which is a fundamental human right in Europe:

> [S]erious questions arise as to the constitutionality of such laws that permit (indeed encourage) the elimination of information from the public domain without proper consideration of the consequences for freedom of expression. Apart from their validity under Member State constitutions, one can doubt the consistency of Internet liability regimes such as those evolving in Europe with Article 10 of the European Convention on Human Rights.

Julià-Barceló & Koelman, *supra* note 289.

the account holder.[309] The First Amendment concerns raised by this legal reform can be best countered by arming content creators with a legal remedy that could be used to punish and deter inappropriate takedown requests, as this Article proposes in Part IV.D.9.[310]

C. *Digital Millennium Copyright Act's Takedown Regime*

Our wished-for ISP regime also would be harmonized with the takedown policy of the DMCA.[311] The DMCA amended the U.S. Copyright Act to adapt to Internet-related technologies.[312] Section 512 of the Act creates a "safe harbor" for ISPs that are providing only

---

309. Jason Schultz, *Copyright Takedown Experiment Reveals Horrible ISP Policies*, *at* http://joi.ito.com/archives/2004/10/20/copyright_takedown_experiment_reveals_horrible_isp_policies.html (Oct. 20, 2004).

310. One commentator stated: "With the European Union's e-commerce directive up for review next year . . . free speech activists will likely press for a 'put-back' provision in any revision of that law or the copyright directive. 'Private censorship sounds a bit hysterical,' [Marsden] said, but that's what the lack of a put-back provision means." COMMUNICATIONS DAILY, Aug. 30, 2004, LEXIS, Nexis Current News Library, Communications Daily File (quoting Christopher Marsden, research officer with Oxford University's Programme in Comparative Media Law & Policy). This Article argues that protections against torts, crimes, and infringement need to be appropriately balanced with the First Amendment. A legal regime which requires notice-based takedown as well as putback will provide protection without unduly chilling free speech.

> ISPs who claimed they couldn't possibly monitor everything said on hosted websites lobbied Congress for protection and, in 1998, President Clinton signed into effect the DMCA. Under Title II of the DMCA, an ISP can avoid financial liability by following the "notice and takedown" provisions, should one of its subscribers offer infringing copy online. These provisions basically state that once an ISP receives notice of the infringement, it must take down the unauthorized material.

Nolo, *When Is an ISP Liable for the Acts of Its Subscribers* (citations omitted), *at* http://www.nolo.com/article.cfm/ObjectID/1902780E-68C9-436B-925AC37E42F4CD71/catID/806B7BA0-4CDF-4221-9230A3135E2DF07A/104/284/205/ART (last visited Mar. 13, 2005); *see* 17 U.S.C. § 512 (2000).

311. Pub. L. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

312. As one court noted:

> "The DMCA was enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability" for "passive," "automatic" actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider. This immunity, however, is not presumptive, but granted only to "innocent" service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 [U.S.C.] § 512(c)(1).

Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1086 (C.D. Cal. 2004) (citations omitted); *see* Digital Millennium Copyright Act, Pub. L. 105-304, § 202, 112 Stat. 2860, 2877–2886 (1998) (codified as amended at 17 U.S.C. § 512).

intermediate and temporary storage of digital copies.[313] ISPs are immunized from copyright infringement claims for four activities: (1) transitory communications;[314] (2) caching;[315] (3) content of websites hosted by the ISP;[316] and (4) information location tools.[317] Section 512(a) of the DMCA limits the liability of a service provider where the ISP merely transmits digital information that may include infringing material. In order to meet the requirements of § 512(a)'s safe harbor, the ISP must meet stringent criteria.[318] Section 512(c) of the DMCA immunizes service providers from copyright infringement claims so long as they do not have actual knowledge of the infringing activity and promptly block allegedly infringing sales once notified.[319] To qualify for such protection, an ISP must meet three requirements: (i) the service provider must either lack both actual knowledge of the infringing activity and awareness of facts or circumstances from which infringing activity should be apparent, or it must promptly, upon gaining such knowledge move to prevent the use of its service to further such infringing activity; (ii) the service provider must not receive a financial benefit directly attributable to infringing activity it has the ability to control; and (iii) the service provider must expeditiously remove material from its service on receipt of an appropriate written notice in order to qualify for safe harbor protection under the DMCA.[320]

The DMCA also tackles the ISPs' responsibility for the content of their websites, bulletin board systems, and other sources of

313. The DMCA created a "safe harbor" for Internet service providers who satisfy the requirements of the statute, which protects them against suits for damages and most injunctive relief. 17 U.S.C. § 512. There are four separate safe harbors within § 512, each with its own separate requirements. *See id.* § 512(a), (b), (c)(1), (d). However, a threshold requirement for any protection by the DMCA is satisfaction of the requirements in 17 U.S.C. § 512(i). Section 512 defines "service provider" as, inter alia, a "provider of online services or network access, or the operator of facilities therefore." *Id.* § 512(k).

314. *Id.* § 512(b).

315. *Id.* § 512(c)(1).

316. *Id.* §512(a).

317. *Id.* § 512(d).

318. *Id.* § 512(a) (noting that ISP is immunized when transmissions are initiated by third parties, copying is done automatically, ISP does not select recipients, copies are not accessible to anyone other than anticipated recipients, and material is transmitted without modification of content).

319. *Id.* § 512(c)(1).

320. *Id.*; Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001) (holding that web site and its employees were protected under safe harbor provision of DMCA against copyright claims and Lanham Act claim was moot because eBay had already removed allegedly false and misleading advertisements); Chilling Effects Clearinghouse, *DMCA Safe Harbor Provisions*, *at* http://www.chillingeffects.org/dmca512 (last visited Mar. 26, 2005).

information.[321] Service providers are not liable for content stored on their systems when they do not have actual or constructive knowledge of the infringing activity.[322] The plaintiff in a copyright infringement action must also demonstrate that the ISP received a financial benefit directly attributable to the infringing activity.[323] The next Part compares the similarities and dissimilarities of our proposed ISP rule with two extant ISP liability regimes already in place, the DMCA and the E-Commerce Directive.

CHART FOUR: COMPARING ISP LIABILITY REGIMES

Feature	**Rustad & Koenig's Distributor with Knowledge Regime**	**DMCA's Online Intermediary Regime**	**E-Commerce Directive's Online Intermediary Regime**
Applicable Law	Applies to all types of illegal content: torts, crimes, and infringement.	Applies only to vicarious or contributory copyright infringement.[i]	Applies to all types of illegal content: torts, crimes, and infringement.[ii]
Duty to Monitor Content	None	None[iii]	None[iv]
Jurisdiction	U.S. Federal Courts[v]	U.S. Federal Courts[vi]	Procedure yet to be determined.[vii]

321. The notice-and-takedown procedure of the DMCA provides ISPs with guidance and a basis for balancing the interests of the complainant and the content provider. A European electronic commerce think tank made a similar point:

> In particular, under the notice and take-down procedure, the law would provide some guidelines as to the form and contents of a notice for an on-line intermediary to act thereon, thus removing the material. Requiring a detailed notice accompanied with sufficient documentation of the claim from the person who says that his rights have been infringed, would help reduce unfounded notices or notices sent [to accomplish] improper objectives[,] such as shut[ting] down debate or prevent[ing] fair competition.

ESPRIT PROJECT 27028, *supra* note 275, at 4.

322. 17 U.S.C. § 512(c)(1)(A)(i)–(iii).

323. *Id.* § 512(c)(1)(B).

ISP Immunity for Transmitting Information	Provides immunity for all caching, conduit, and hosting activities[viii] ISPs have immunity as publishers and as distributors unless they fail to act expeditiously after actual notice of illegal content.	Provides immunity from damages for caching, conduit, and hosting activities;[ix] and also for contributory or vicarious copyright infringement so long as safe harbor requirements are fulfilled.[x]	Provides immunity for all conduit activities: caching,[xi] conduit,[xii] and hosting data.[xiii]
Conditions for ISP "Safe Harbor"	We adopt the DMCA's notice and takedown regime for all infringement, torts, and crimes.[xiv]	No immunity without registration of agent with U.S. Copyright Office.[xv]	No registration requirement and no procedures have been developed for takedown and put-back demands.[xvi]
Limited Liability	Imposes ISP liability only if provider has actual notice[xvii] of ongoing illegal activity.[xviii]	To qualify for immunity, ISP must remove material upon actual notice[xix] by copyright owner.[xx]	Imposes ISP liability for illegal content where ISP has actual or constructive notice of illegal activity.[xxi] Imposes no duty to monitor, so it is unclear what

			constitutes constructive notice.[xxii]
Registration and Notice	Our unified proposal extends DMCA's procedures to torts and crimes.[xxiii]	ISP agent's contact information must be posted on the website and with the U.S. Copyright Office.[xxiv] Complainants must provide ISPs with verifiable contact information.[xxv]	The Directive imposes no specific registration or notice requirement that would give the ISP guidance on when to act.
Remedies Against ISP	Notice, Takedown & Put-back: Monetary Damages.	Notice,[xxvi] Takedown & Put-back[xxvii]	Notice, Takedown, & Put-back: Damages.[xxviii]
Safeguards Against Bad-Faith Requests	Compensatory and Punitive Damages for frivolous or bad faith takedown demands	Monetary damages imposed on copyright owner who provides false or misleading takedown notice to ISP.[xxix]	No Provision[xxx]

D. Comparing Takedown Regimes

Chart Four compares and contrasts our online intermediary proposal with the takedown provisions of the DMCA and the E-Commerce Directive. Under our legal reform, ISPs would be liable only for failing to act swiftly in blocking or removing content known to be a venue for an ongoing tort. Content creators would have a right to a hearing in any U.S. federal court to challenge inappropriate or frivolous takedown or

put-back orders.[324] This tort reform will harmonize § 230 with the takedown regime already in place for U.S. copyright infringement claims.[325]

Takedown is already the de facto enforcement tool of choice used by ISPs to police the Internet.[326] Corporate Internet actors already recurrently remove objectionable content as a means of self-help. Microsoft, for example, recently took down a Windows news site for nearly twenty-four hours after a provider accused the site of infringing its copyrights.[327] Powerful entertainment industry stakeholders have on occasion taken down material even when they had no legal right to do so. The Recording Industry Association of America (RIAA) has initiated a number of erroneous DMCA demands against individuals as well as websites.[328] For example, "[s]even record labels mistakenly sued a 65-year-old Massachusetts woman for copyright infringement."[329]

Online intermediaries complain about inappropriate demands. "In 2002, Pacific Bell Internet Services and its affiliates were given more than 16,700 DMCA notices by RIAA agent MediaForce; in July 2003, RIAA attempted to serve more than 200 subpoenas through various affiliated entities."[330] An online pornography website sent a DMCA demand to an ISP "demanding identities of alleged infringers at 59 different dynamically assigned IP addresses, then dropped the subpoena when Pacific Bell announced its intent to challenge its enforcement."[331] A recent study of the DMCA concludes that takedown orders have been

---

324. This procedure is necessary in tort cases where the ISP cannot clearly ascertain whether an information tort has been committed. Most cybertort injuries are based on fraud or other intentional torts, which would not require a hearing.

325. No compelling reason exists to have absolute immunity from tort liability but limited liability from copyright infringement. The "notice, takedown, and put-back" proposal for torts is carefully balanced to prevent ISPs from being overrun by frivolous requests. In our proposal, the ISP has no duty to monitor content and must act only after receiving actual notice by a registered complainant. Frivolous takedown or put-back requests may subject the complainant to a lawsuit for punitive damages in egregious circumstances.

326. Joe Wilcox, *Microsoft Speaks, Site Goes Dark*, CNETNews.com, Mar. 10, 2003, *available at* http://news.com.com/2100-1025-991624.html?tag=fd_lede1_hed.

327. *Id.*

328. *See* Declan McCullagh, *RIAA Apologizes for Erroneous Letters*, CNETNews.com, *at* http://news.com.com/RIAA+apologizes+for+erroneous+letters/2100-1025_3-1001319.html (May 13, 2003).

329. Electronic Freedom Foundation, *Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands*, *at* http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php (last visited Apr. 7, 2005).

330. *Id.*

331. *Id.*

misused:

> The DMCA has been used to invade the privacy of Internet users, harass Internet service providers, and chill online speech. The subpoena and takedown powers of Section 512 are not limited to cases of proven copyright infringement, and are exercised without a judge's review. . . . Judicial oversight could curb these abuses without interfering with copyright enforcement.[332]

Given this pattern of known abuse, it is imperative to have safeguards against bad faith, frivolous, or erroneous takedown requests. Our proposal addresses the problem of flawed takedown requests by providing judicial oversight and remedies with teeth. This new ISP rule gives content creators the right to a federal court hearing to promptly reverse unsound takedown orders. Persons or entities will be liable for financial penalties, including punitive damages, when they make a strategic takedown demand that is calculated to injure competitors or is otherwise in bad faith.[333] The DMCA provides an excellent blueprint for our proposal because it makes complainants accountable for any actual or consequential damages to the content creator for making a material misrepresentation to a provider.[334]

1. The Applicable Law

This Article proposes to utilize the same rule for intellectual property infringement as the rule currently followed by the DMCA.[335] It applies the "distributors with knowledge" rule to all civil liabilities of online intermediaries, not just those liabilities imposed by tort law. The proposed regime will restore balance in the law of online intermediaries by imposing limited liability on ISPs for failing to take down infringing or tortuous content. Content creators who are victimized by bad faith takedown demands will have recourse in the form of actual damages and punitive damages, a remedy not available under either the DMCA or the E-Commerce Directive.

---

332. *Id.*

333. *See* MORRISON & FOERSTER, *supra* note 297, at 4 (stating E-Commerce Directive contains similar provision).

334. *Id.*

335. *See* 17 U.S.C. § 512 (2000).

2. *No Duty to Monitor Content*

This Article's projected ISP rule does not impose a duty on service providers to monitor content, which is consistent with the provisions of the CDA, DMCA, and the E-Commerce Directive. The E-Commerce Directive makes it clear that the provider has no affirmative duty to monitor content.[336] However, article 15(2) of the Directive allows the Member States to enact legislation to require the provider to notify law enforcement when it determines that there are illegal activities on its service.[337] The DMCA also does not require ISPs to monitor content, but they must remove content upon discovery of the infringement.[338]

Under this Article's proposal, an online intermediary that learns of ongoing infringing, tortious, or criminal material must take prompt action as soon as it learns of objectionable material.[339] Our proposal is harmonized with the DMCA rule that providers must take prompt remedial measures when they receive actual notice of infringing material, even if this occurs prior to a formal takedown notice.[340] Our reform adopts the general notice and procedural protections of the DMCA and simply extends the duty of ISPs from removing infringing materials to removing or disabling tortious content upon discovery.[341] The ISP, in other words, is divested of its federal immunity at the point that it obtains actual notice or acquires actual knowledge of infringement and fails to expeditiously remove or disable objectionable content.[342]

---

336. E-Commerce Directive, *supra* note 27, at art. 15(1), at 13 (member states shall not impose a general obligation on members).

337. Article 15(2) states that:

> Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

E-Commerce Directive, *supra* note 27, at art. 15(2), at 13.

338. 17 U.S.C. § 512.

339. Neither the DMCA nor the E-Commerce Directive addresses immunity for criminal activity. Immunity is not available for violations of federal criminal statutes under the CDA. 47 U.S.C. § 230(e)(1) (2000).

340. The DMCA's protection of an innocent service provider under 17 U.S.C. § 512(c)(1) "disappears at the moment the service provider becomes aware that a third party is using its system to infringe." Upon receiving notice, the DCMA shifts responsibility to the service provider to disable the infringing matter, preserving the strong incentives for prompt remedial action. *See* Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1086 (C.D. Cal. 2004).

341. *See* 17 U.S.C. § 512(c)(1)(A)(iii); *id.* § 512(d)(1)(C).

342. In most instances, the ISP will acquire actual notice of infringement or an ongoing tort by

3. *Federal Court Oversight of Takedown & Put-Back*

Federal court oversight is necessary to put a stop to unwarranted takedown demands based on general, vague, or inaccurate allegations. We believe that our proposal to extend the DMCA framework to information torts and other illegal activities will not inundate the courts with new cases[343] nor pose difficult transition problems for the federal courts.[344] Since 1998, the federal district courts have decided only a handful of cases construing the DMCA's takedown procedures, even though the DMCA provides content providers with the right to a federal court hearing.[345]

As shown in Part I, most cyberlaw cases are already decided in federal courts, as are all copyright infringement disputes under the DMCA. In many instances, takedown demands will arise out of disputes over federal statutory rights for intellectual property rights. Ensuring the right to a federal district court hearing appropriately balances the rights of content creators, consumers, and other Internet stakeholders. Under our proposal, federal district courts will have jurisdiction over claims that ISPs failed to satisfy the conditions for a safe harbor.[346] The federal courts' experience in deciding DMCA liability cases will prove invaluable for establishing the parameters for takedown procedures, put-back appeals, and other embryonic problems.

One of the advantages of adopting the DMCA's methodology for

---

receipt of a complaint. Our proposal tracks the DMCA's procedure, which requires the complainant to provide sufficient information to identify infringing material and contact the infringing party. *See id.* § 512(c)(3)(A)(iv).

343. A federal district judge commented that our proposed takedown and put-back proposal calling for federal court hearings might swamp the court's already burdensome docket. Memorandum from Judge Edward F. Harrington to Michael L. Rustad & Thomas H. Koenig (Oct. 29, 2004) (commenting on draft of Article) (on file with Authors). Federal courts already handle DMCA "takedown" and "put-back" procedures, and their increasing expertise in this field makes them the best possible tribunals. We do not envision a floodgate of distributor-with-knowledge lawsuits because most takedown requests will be obvious tortious or criminal activities not requiring a judicial opinion. The federal court would only hear a case in which the content provider challenges the decision to take down content.

344. One potential problem of our unified procedure is that, on its face, it appears to federalize tort law for cyberspace. The federal courts may wish to remand selected issues of tort law to the state's highest court just as they often do in diversity cases.

345. A LEXIS/NEXIS search, conducted on Jan. 12, 2005, of all federal and state cases, uncovered five decisions discussing DMCA takedown procedures.

346. *See, e.g.*, Ellison v. Robertson, 357 F.3d 1072, 1074 (9th Cir. 2004) (affirming summary judgment on vicarious liability; remanding for trial on contributory infringement issue based on DMCA safe harbor provisions).

takedowns and put-backs is that there is a well-established procedure for resolving disputes between content providers, websites, and service providers, as illustrated in the recent case of *Rossi v. Motion Picture Ass'n of America, Inc.*[347] In *Rossi*, a website owner appealed a decision of the federal district court granting summary judgment to the motion picture trade association in a tort action.[348] The plaintiff owned and operated the "internetmovies.com" website.[349] The plaintiff's website encouraged subscribers to: "Join to download full length movies online now! new movies every month."[350] The Motion Picture Association of America (MPAA) has a mission that includes preventing unauthorized copying, transmittal, or other distribution of the movie studios' motion pictures.[351] After viewing the website, the MPAA believed that illicit copying of movies was taking place, and it sent a DMCA takedown demand to both the website and its service provider.[352]

The ISP then sent a DMCA notice to the website, stating that the website would be shut down.[353] The plaintiff responded by finding "a new ISP to host internetmovies.com."[354] The plaintiff then sued the MPAA in federal court on a variety of tort claims, including tortious interference.[355] The federal court ruled that the MPAA had complied with the DMCA's notice-and-takedown procedure and entered summary judgment against the plaintiff on all counts.[356] The federal appeals court affirmed the lower court's ruling that the MPAA acted in good faith.[357]

4. *Immunity for Transmitting Content*

Our ISP reform confers immunity on all online intermediaries for purely conduit activities, whether the content is challenged on proof that it is infringing, tortious, or criminal. Copyright owners must abide by the

347. 391 F.3d 1000 (9th Cir. 2004).

348. *Id.* at 1002 (describing complaint for tortious interference of contract, defamation, and intentional infliction of emotional distress in association's takedown request under DMCA).

349. *Id.* at 1001–02.

350. *Id.* at 1002.

351. *Id.*

352. *Id.*

353. *Id.*

354. *Id.*

355. *Id.*

356. *Id.*

357. *Id.* at 1006 (affirming district court's finding that no issue of material fact existed as to good faith belief).

DMCA notice requirements to compel ISPs to remove or disable infringing content.[358] Article 12 of the E-Commerce Directive exempts ISPs for mere conduit activity.[359] ISPs must act reasonably in taking down infringing content once they receive notice. Our unified ISP proposal tracks the DMCA in imposing a registration requirement on intermediaries claiming immunity for these activities.[360]

5. *Conditions for ISP Safe Harbor*

ISPs should not be shielded from liability unless they fulfill all of the procedural steps necessary to qualify for a safe harbor. Our service provider reform proposal incorporates the DMCA's registration and notice requirements. ISPs are not entitled to a "safe harbor" unless they register contact information with the U.S. Copyright Office. In addition, the online intermediary must: (1) have no actual knowledge of, or financial benefit[361] from, the infringing, tortious, or illegal activity; (2) have no role in modifying or creating the objectionable content; (3) post a conspicuous notice on its website informing users of the procedure for making takedown requests; (4) appoint an agent to deal with takedown and put-back requests; (5) provide a verifiable telephone number, mailing address, and e-mail address for complaints about illegal or objectionable content; and (6) register its website and agent contact with an appropriate government entity.[362] These well-honed procedures will be extended from copyright infringement cases to all forms of objectionable conduct, including cybertorts.

---

358. 17 U.S.C. § 512(c)(3)(A) (2000) (stating that to be effective, notification must be written communication to designated agent of service provider, containing physical or electronic signature of person authorized to act for copyright owner; identification of material claimed to be infringing, information sufficient to permit service provider to contact complaining party; statement that complaining party has good faith belief that material is not authorized by copyright owner; and statement made under penalty of perjury that notification is accurate).

359. E-Commerce Directive, *supra* note 27, at art. 12, at 12–13 (immunizing ISPs from damages liability for content transmitted by third parties so long as ISP does not initiate transmission, select recipient, or select or modify information); *see also id.* at art. 13, at 13 (immunizing liability for caching activity); *id.* at art. 14, at 13 (immunizing liability for hosting activity).

360. As with the DMCA, our proposal confers immunity on search engines such as Google, Yahoo!, and Excite for references or links to infringing materials. *See* 17 U.S.C. § 512(d).

361. Financial benefit in this context means that the ISP profits directly from the distribution, transmission, or storage of the actual content, as opposed to being a passive conduit where it enjoys immunity.

362. This Article's proposal's ISP registration requirement mirrors the DMCA's § 512 procedures.

6. *ISP Liability*

The foundation of our reform proposal is to institute a limited liability for ISPs that strips them of distributor immunity once they have actual notice of ongoing torts, crimes, or other illegal activities on their services and fail to expeditiously remove objectionable content. Our ISP regime is harmonized with the Directive that has been in place throughout Europe since 1998. Our proposal adopts the conduit liability rules already in place under the E-Commerce Directive as well as the DMCA. Article 12 of the Directive immunizes ISPs when they are acting as "mere conduits," which means that they do not "initiate the information,"[363] "select the receiver of the transmission,"[364] or "select or modify the information contained in the transmission."[365]

The Directive's ISP immunity extends to all housekeeping and administrative tasks in the transmission of information including caching,[366] hosting,[367] and other acts of transmission, so long as they are not deemed content creators.[368] ISPs are liable for not expeditiously removing content that constitutes infringement or for torts or crimes after they acquire notice of objectionable content,[369] but they have no obligation to monitor content.[370] Our unified ISP reform mirrors the E-Commerce Directive because it applies to all takedown requests, whether classified as copyright infringement or other illegal content. Our law reform also adopts the E-Commerce Directive's rule that ISPs have no general obligation to monitor objectionable content.

---

363. E-Commerce Directive, *supra* note 27, at art. 12(1)(a), at 12.

364. *Id.* at art. 12(1)(b), at 12.

365. *Id.* at art. 12(1)(c), at 12.

366. *Id.* at art. 13, at 13.

367. *Id.* at art. 14, at 13.

368. Article 12 states:

> The acts of transmission and of provision of access referred to . . . include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

Id. at art. 12(2), at 12.

369. "The directive covers all forms of IP, including copyright, patent and trademark, but would permit member states to go beyond it by enacting greater protections for rights holders in business tort cases and licensing disputes." *Controversial Proposal*, *supra* note 300, at 153.

370. E-Commerce Directive, *supra* note 27, at art. 15, at 13 (noting that ISPs have no general obligation to monitor services provided by ISP, such as e-mail communications).

7. *Our Proposed Rule for ISP Notice*

The Directive is a sweeping set of general legal principles rather than the detailed guidance needed to implement a workable ISP takedown policy. The Directive provides little by way of practical advice to ISPs on how to administratively handle takedown and put-back. The Directive, for example, does not address the issue of whether a content creator is entitled to notice prior to its content being removed. The Directive does not require Member States to adopt enabling legislation requiring ISPs to contact law enforcement when they become aware of illegal activities on their services.[371] Similarly, the E-Commerce Directive does not provide a specific takedown framework, nor does it specify the "circumstances and requirements under which 'private notices' [are] given to host service providers."[372]

The E-Commerce Directive's failure to address the relative rights of content creators to dispute takedown requests is troubling. The Directive does not even require that third-party content creators be given notice that their materials are being taken down; it leaves such rules to the Member States. Our reform gives ISPs the specific guidance that they need before taking down objectionable content, balancing the protection of the public with the uniquely American concern for free expression.[373]

Shackling the First Amendment would be a cyberspace travesty. However, the First Amendment is not an absolute, even for Internet speakers.[374] There is no First Amendment right to commit tort injuries

371. E-Commerce Directive, *supra* note 27, at art. 15(2), at 12 (stating that Member States may establish procedures by which providers inform law enforcement authorities of suspected illegal activities).

372. Julià-Barceló & Koelman, *supra* note 289.

373. The vague takedown procedures of the E-Commerce Directive have been criticized as creating a legal environment where ISPs take down content without sufficient investigation. A Dutch civil rights group did an experiment in which they posted an 1871 document not protect by copyright on accounts with ten different ISPs. They next e-mailed takedown notices to each ISP claiming that they were the valid copyright holder of the document and demanding that it be taken down. Seven of the ten ISPs removed the "objectionable" material within hours without even informing the account holder. Schultz, *supra* note 309.

374. As Professor Lambert reminds us, there are no constitutional absolutes:

> The roster of such limitations [to the First Amendment] is not only numerous but formidable. They include obscenity, perjury, deceit, libel (private as well as political), invasion of privacy, false advertising, breach of express warranty, disparagement, injurious falsehood, passing off, espionage, state secrets, contempt of court by epithet and antic and publication, tort of "Outrage," misappropriation of trade secrets, misleading signals by a driver about to make a turn, false reassurances that dangers do not exist, violations of anti-dueling statutes by use of abusive and insulting language, "incitements" to immediate breaches of the peace, et cetera, et cetera.

with impunity. Free speech is not a hunting license that immunizes those who misappropriate personal information, intrude on privacy, distribute child pornography, incite hackers, and engage in shabby trade practices such as indiscriminately consuming bandwidth with an ocean of spam e-mail.

Under our reform proposal, complainants requesting that objectionable material be blocked or removed must provide certifiable contact information as well as comply with a prescribed notice to the ISP.[375] Complaints must document and warrant that the content is infringing, illegal, or tortious. In addition, the ISP is required to give notice to the target of the complaint. The ISP is not required to give notice prior to takedown, but it must convey notice if it makes a decision to remove or block content.

8. *Remedies Against Negligent ISPs*

Our proposed ISP rule requires complainants to identify specifically which website materials constitute ongoing torts or infringe the intellectual property rights of owners. Once the ISP has actual notice of illegal activity, it has a duty to expeditiously remove or block access to the materials. ISPs may acquire this actual notice of illegal activity prior to a complaint although they have no affirmative duty to monitor their services. Both the E-Commerce Directive and the DMCA have put-back procedures to restore content by providing a prescribed notice. The ISP's failure to comply with the DMCA's registration, notice, and put-back procedures exposes them to the possibility of monetary damages or equitable remedies.[376] Our proposal extends these procedures beyond

---

Thomas F. Lambert, Jr., *Tort Law*, 37 ATLA L.J. 32, 65 (1978).

375. In the unified ISP regime, the complaint is required to make a statement of the accuracy of the underlying facts in its complaint under penalty of perjury. Secondly, the complainant must attest that it has the authority to act on behalf of the plaintiff. The requirement that the complainant register is based largely on the DMCA takedown procedure. *See* 17 U.S.C. § 512(c)(3)(A)(vi) (2000) (noting that proposed ISP liability rule requires that complainant provide verifiable address and contact information); *id.* § 512(c)(3)(A)(i). Whereas the DMCA requires the complaint to provide sufficient information to identify infringing material, the new ISP rule would require sufficient facts to establish a prima facie case for ongoing infringement, ongoing torts, or crimes. *Cf. id.* § 512(c)(3)(A)(iii). The new ISP rule requires the complainant to attest to the accuracy of the notice as well as the underlying facts. The DMCA takedown rule requires owners to attest to a good faith belief in the notice. *Id.* § 512(c)(3)(A)(v). In addition, the complaints must attest to the accuracy of the claim of infringement and that the complainant is an authorized agent for the copyright owners. *Id.* § 512(c)(3)(A)(vi).

376. *See generally* Kenneth D. Salomon, *Distance Education at the Dawn of the Digital Millennium Copyright Act*, *at* http://web.archive.org/web/20041020025702/

copyright infringement to information torts as well as other illegal activities.

9. *Safeguards Against Bad-Faith Requests*

Our suggested ISP reform implements the DMCA's safeguards against bad-faith or frivolous takedown requests. Congress created a framework of deterrence against bad-faith takedown requests including the possibility of damages, costs, and attorneys' fees against bad-faith claimants.[377] ISPs, on the other hand, enjoy limited liability for inappropriate takedowns or disabling of posted content, unless their bad faith is proven or glaring misrepresentations are apparent in the takedown notice.[378]

The notice requirement of our proposed ISP rule extends the procedures of § 512 of the DMCA to all ongoing torts, crimes, and intellectual property infringement. The targeted content creator has a fourteen-day window to challenge or request reinstatement of the material blocked or taken down.[379] Unlike the DMCA, complaints that instigate takedown requests through misrepresentations or in bad faith are required to indemnify the ISP as well as the blameless target of the request. The goal of these proposals is to punish and deter those who demand abusive or bad-faith takedowns.

Both the E-Commerce Directive and the DMCA have similar put-back procedures to restore content by providing a prescribed notice.[380] The DMCA calls for those who request the takedown or put-back procedures to register with the U.S. Copyright Office.[381] The DMCA and the E-Commerce Directive both hold a person liable who makes a takedown or put-back demand that is in bad faith.[382] Under the DMCA, a

---

http://www.pbs.org/als/agenda/articles/digimilli.html (last visited Apr. 25, 2005).

377. 17 U.S.C. § 512(f).

378. *Id.* § 512(g)(1).

379. *See id.* § 512(b)(2).

380. The E-Commerce Directive "contains a put-back regime similar to that in the DMCA, where the person whose content is alleged to be an infringement may have the allegedly infringing content put back by providing notice in the form described in the [Directive]." MORRISON & FOERSTER, *supra* note 297, at 4; Ecomlex, *Implementation of the E-Commerce Directive—Status as of 17 January, 2002* (reporting Finland's implementation of E-commerce Directive), *at* http://www.ecomlex.com/documents/FinlandDir.pdf (last visited Mar. 17, 2005).

381. 17 U.S.C. § 512(c)(2) (specifying information that designated agent must post with Copyright Office to qualify for limitations on secondary copyright liability).

382. MORRISON & FOERSTER, *supra* note 297, at 4.

person or entity making a material misrepresentation to a provider is liable for any actual or consequential damages to the content creator.[383]

In summary, our "notice, takedown and put-back" regime would apply to torts, crime, and infringement for all branches of intellectual property law. The proposal follows the DMCA's paradigm by requiring ISPs to expeditiously remove or block illegal or tortious content upon actual notice by a registered complainant. However, we strongly favor the right of providers to file damages lawsuits against those parties that initiate bad faith or frivolous takedown or put-back requests. Content providers targeted by frivolous takedown requests need remedies with teeth for use against bad faith complainants.

At present, the E-Commerce Directive does not give content creators the right to a hearing, which forces ISPs to respond promptly to complaints about content without input from the other side. Our proposal provides far greater guidance for ISPs than the Directive. Our ISP reform proposal provides aggrieved content creators or ISPs victimized by inappropriate takedown requests with the right to have a federal court hearing where legal or equitable remedies may be obtained. The E-Commerce Directive, in contrast, has not provided for any judicial forum for adjudicating disputes over takedown and put-back.

Our proposal is designed to be a modest first step in blazing a new trail for the development of cybertort law. If the distributor with notice rule applied to online stalking, for example, ISPs would have incentives to create new authentication technologies and conduct audits of the cyberstalker's Internet accounts and records of his online activities that would be helpful in either a criminal prosecution or a civil action. A robust cybertort regime will provide legal certainty by encouraging content providers, online intermediaries, and ISPs to work together in providing a safer Internet.

CONCLUSION

The rapid pace of technological change has exposed a fundamental weakness in the American civil justice system. The present legal regime of self-regulation by Internet stakeholders provides no favorable remedies against ISPs for their direct negligence or for failing to prevent crimes or torts against their customers. At present, the law of cybertorts does not require ISPs to take down defamatory material, no matter how injurious. There is no duty of care for ISPs to refrain from reposting

383. *Id.*

injurious communications or mitigating ongoing tortious activities on websites so long as third parties supplied the illegal content. No search engine or service provider has a duty to disable fraudulent advertisements, even if it has notice of crimes being committed through its online sales websites.

The history of tort law is composed of landmark judicial decisions that breached the citadel of regressive precedents. Just as many common-law barricades to tort recovery were consigned to the ashbin of history after World War II,[384] so must the judicially expanded § 230 obstructions to recovery be discarded. Imposing ISP liability for notorious websites that harm the public interest reallocates some of the costs of injury based on the least cost avoider principle. Today's judiciary needs to be bolder in carving out cybertort duties to compensate the victims of Internet crimes and torts.

Greater accountability in cyberspace should be achieved by restoring the common law distinction between publishers and distributors, which has been eradicated by recent court decisions construing § 230. Under our online intermediary standard, ISPs and other intermediaries would continue to enjoy immunity for conduit activities. However, they would be subject to tort liability for third party crimes and torts under a reinvigoration of the distributor standard for all Internet torts.

Congress should amend § 230 to faithfully reflect the need to balance free expression with greater ISP accountability. This downsizing of the entrenched CDA rule is only the first step toward developing a negligence-based regime that will reduce the cost of injury in cyberspace by imposing new duties on ISPs. A Department of Justice attorney specializing in cybercrimes acknowledges that consumers have no real protection from a wide variety of Internet misdeeds:

> Benefiting from the confusion, many cyber-predators exploit gaps in the law, test its limits, and hide behind conflicting definitions of criminal activity. Identity predators, for example, abuse lax information-sharing policies to commit identity fraud. Cyberstalkers track their victims online, sending offensive e-mails or menacing messages using Instant Messaging technology. Spammers not only bombard users with unsolicited

384. Liability-limiting rules, defenses, and immunities "retreated like a melting glacier" in the post-World War II period. Robert L. Rabin, *The Historical Development of the Fault Principle: A Reinterpretation*, *in* PERSPECTIVES ON TORT LAW 44, 68 (Robert L. Rabin ed., 2d ed. 1983). *See generally* Rustad & Koenig, *supra* note 278 (discussing in depth expansion and contraction of tort rights over course of U.S. history).

> junk e-mail, but can also spread destructive computer viruses—like the SoBig.F virus—within messages that have misleading subject lines.[385]

ISPs such as America Online are no longer delicate infants that need absolute immunity in order to survive. Crafting new duties for ISPs will restore the ability of tort law to go forward to mediate the new risks and opportunities facing consumers in cyberspace.

---

i. Copyright infringement occurs when a defendant violates one of the exclusive rights of the copyright holder. *Id.* § 501(a). A plaintiff can establish direct infringement by demonstrating that a defendant used the copies in any of the ways described under 17 U.S.C. § 106, which include: (1) reproduction of the copyrighted work; (2) preparation of derivative works based upon the copyrighted work; (3) distribution of copies of the copyrighted work to the public by sale or other transfer of ownership; or (4) display of the copyrighted work publicly. *Id.* § 106. To be liable for direct infringement, one must "actively engage in" and "directly cause" the copying. *See generally* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). In contrast, contributory infringement requires proof of infringing activity and the defendant's material contribution to the infringement. *See* Sega Enters. Ltd. v. Maphia, 948 F. Supp. 923, 932–33 (N.D. Cal. 1996).

ii. The E-Commerce Directive provides that:

> Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

E-Commerce Directive, *supra* note 27, at art. 15(2), at 12.

iii. The DMCA imposes no duty on the service provider but rather places the burden on the copyright owner to monitor the Internet for potentially infringing sales. *See* 17 U.S.C. § 501(a).

iv. Article 15 states that providers have no general obligation to monitor and prohibits member states from enacting legislation requiring ISPs to monitor content. *See* E-Commerce Directive, *supra* note 27, at art. 15(1), at 12 ("Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.").

v. At present, no international treaty or entity governing the Internet has been established. As our

---

385. Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, ¶ 8, *available at* http://stlr.stanford.edu/STLR/Articles/04_STLR_2/article_pdf.pdf (last visited Mar. 26, 2005).

empirical study demonstrates, federal courts decide most U.S. Internet disputes and are the best-qualified legal decisionmaker.

vi. Federal courts have jurisdiction to consider federal copyright claims. 17 U.S.C. § 512.

vii. Article 3(1) of the E-Commerce Directive requires that:

> Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicabl in the Member State in question which fall within the coordinated field. (requirements laid down in the national system applicable to Information Society service providers in the light of the present Directive).

E-Commerce Directive, *supra* note 27, at art. 3(1), at 9; *see* EU Electronic Commerce Directive: Jurisdictional Aspects, *at* http://www.smaldonado.com/marcos/docs/pi_di00_cl_eu_en.html (last visited March 16, 2005); *see also* Julià-Barceló & Koelman, *supra* note 289 (arguing that E-Commerce Directive has not developed specific rules for implementing E-Commerce Directive). Similarly, it is unclear how jurisdictional issues would function in this uncertain legal environment. *See generally* Council Regulation 44/2001/EC of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgements in Civil and Commercial Matters, 2001 O.J. (L 12) 1, *available at* http://www.ip-firm.de/eugvue_e.pdf (last visited Apr. 25, 2005).

viii. The proposed regime adopts the same conduit immunity rule as implemented by the DMCA and E-Commerce Directive. 17 U.S.C. § 512; E-commerce Directive, *supra* note 27, at art. 12–14 at 12–13.

ix. Section 512 of the DMCA, entitled "Limitations on Liability Relating to Material Online," immunizes service providers against monetary or injunctive actions for "transitory digital network communications." 17 U.S.C. § 512(a). This section gives service providers immunity for the transmission of material "initiated by or at the direction of a person other than the service provider" so long as activities such as transmitting, routing or storing data are an "automatic response to the request of another person." *Id.* § 512(a)(1), (3). There is no conduit immunity if the provider selects recipients "except as an automatic response to the request of another person." *Id.* § 512(a)(3). A provider is stripped of its immunity if it makes a copy of copyrighted material for a purpose other than conduit activity. *Id.* § 512(a)(4). Similarly, there is no ISP liability for "system caching" that arises out of either intermediate or temporary storage of material. *Id.* § 512(b)(1). All of these conduit immunities are conditional on the assumption that the provider does not modify content. *Id.* § 512(a)(5), (b)(2). Finally, the ISP is not liable for information residing on systems or networks at the direction of users. *Id.* § 512(c).

None of this immunity is available to service providers unless they comply with the DMCA safe harbor provisions in § 512(b)(2). Providers must designate an agent "to receive notifications of claimed infringement." *Id.* § 512(c)(2). Providers must make this information available both on their websites and by providing the same information to the U.S. Copyright Office. *Id.* The specific elements of notification require that the complainant provide "[a] physical or electronic signature of a person authorized to act on behalf of the [copyright] owner allegedly infringed." *Id.* § 512(c)(3)(A)(i). A complainant also must identify the copyrighted work that is claimed to have been infringed. *Id.* § 512(c)(3)(A)(ii). The person or entity claiming that material is infringing must give the ISP the necessary information to locate the objectionable material. *Id.* § 512(c)(3)(A)(iii). The person or entity initiating takedown must give a physical address, telephone number, and e-mail address where they may be contacted. *Id.* § 512(c)(3)(B)(A)(iv). The complainant must attest to a "good faith belief that use of the material" is not authorized. *Id.* § 512(c)(3)(A)(v). Finally, a complainant who makes a bad-faith claim is subject to perjury. The complainant must attest to the accuracy of the information in the takedown request. *Id.* § 512(c)(3)(A)(vi). Section 512(g)(2)(E) requires the service provider to "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement." *Id.* § 512(g)(2)(E). Accordingly, the DMCA, unlike the Directive, clarifies when ISPs are liable for infringement.

x. Congress intended the DMCA's safe harbor for ISPs to be a floor, not a ceiling, of protection:

> Congress said nothing about whether passive ISPs should ever be held strictly liable as direct infringers or whether plaintiffs suing ISPs should instead proceed under contributory theories. The DMCA has merely added a second step to assessing infringement liability for Internet service providers, after it is determined whether they are infringers in the first place under the preexisting Copyright Act. Thus, the DMCA is irrelevant to determining what constitutes a prima facie case of copyright infringement.

CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004). "In order to enjoy the safe harbor provided by §512(c), the ISP must also fulfill other conditions imposed by the DMCA." *Id.* at 552 (citing 17 U.S.C. § 512(c)(i)).

xi. Article 12 provides immunity for mere conduits:

> 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
>
> (a) does not initiate the transmission;
>
> (b) does not select the receiver of the transmission; and
>
> (c) does not select or modify the information contained in the transmission.
>
> 2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

E-Commerce Directive, *supra* note 27, at art. 12, at 12–13.

xii. *Id.*

xiii. Article 13 of the E-Commerce Directive provides immunity for caching:

> 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
>
> 2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Id. at art. 13, at 13.

xiv. One unsettled question is where takedown requests should be submitted outside the realm of infringement claims. We suggest making the U.S. Copyright Office the sole registration entity for all objectionable content because its staff is familiar with the detailed procedures of the DMCA that need be only slightly modified for torts and crimes. For example, the language about ISP Liability Safe Harbors in § 512 can be easily adapted from infringement to defamation. The same rules

immunizing ISPs for passive transmissions, cached copies, user-stored information, information and information location tools apply irrespective of whether the objectionable conduct is infringing or tortious. The DMCA rule that immunizes ISPs takedown activities where they are in good-faith compliance with prescribed procedures is a good model to adapt for torts and other illegal activity. The DMCA's rules on repeat infringers should also be extended to recidivist tortfeasors such as the fraudulent seller in our Yahoo! Example, as well as ongoing defamers or invaders of privacy.

xv. 17 U.S.C. § 512(c)(2).

xvi. *See generally* E-Commerce Directive, *supra* note 27.

xvii. The proposed ISP regime requires that complainants provide verifiable contact information as well as a notice containing evidence of infringing, tortious or criminal activities. The DMCA takedown regime requires the complainant to provide his or her name, address, and electronic signature. *See* 17 U.S.C. § 512(c). In addition, our proposal requires more detailed information on the nature of the tort or infringement.

xviii. The "actual notice" requirement is designed to protect ISPs from having a de facto duty to monitor or screen content, thus balancing liability concerns with the First Amendment.

xix. The DMCA's takedown procedure applies only if the ISP has actual notice. Section 512(b)(2)(E) imposes the duty to remove or block access only if:

> (i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and (ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

17 U.S.C. § 512(b)(2)(E). Section 512(c)(3) requires that the accusing party identify the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, provide a representative list of such works at that site. The notification must contain a statement that the information in the notification is accurate, and, under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. *Id.* § 512(c)(3)(A)(vi).

xx. *See* 17 U.S.C. § 512(c)(3)(A)(i).

xxi. *See* E-Commerce Directive, *supra* note 27, at art. 14, at 13 (noting obligation of provider, "upon obtaining such knowledge or awareness, [to act] expeditiously to remove or to disable access to the information"); *see also id.* at art. 14(3), at 13 (stating that Article 14 "shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information").

xxii. Article 15 of the E-Commerce Directive expressly states there is no duty to monitor content, so it is unclear what factual circumstances would constitute constructive notice. *Id.* at art. 15, at 13. Unfortunately, there is no case law and little by way of commentary on specifics of this regime.

xxiii. This procedure mirrors the DMCA rule that ISPs must "designate[] an agent to receive notifications of claimed infringement" of their intellectual property rights." 17 U.S.C. § 512(c)(2). In addition, ISPs are required to file the appointed agent's name, address and other contact information with the U.S. Copyright Office. *Id.* Finally, this information must be posted prominently on the ISP's services. *Id.* Congress could, at its discretion, make the Copyright Office the designated repository for appointed agents covering areas beyond copyright infringement. The U.S. Copyright Office has a mechanism for registering agents that could easily be adapted to complaints for other intellectual property infringement, ongoing torts, crimes or other illegal

materials. It would be desirable for one government entity to handle all agent registrations. *Id.* § 512(c). The U.S. Copyright Office maintains a website list of all service providers who have filed designations of agents for notification of claims of infringement pursuant to § 512(c) of the Copyright Act. Directory of Service Provider Agents for Notification of Claims of Infringement, *at* http://www.copyright.gov/onlinesp/list/index.html (last visited March 20, 2005).

xxiv. 17 U.S.C. § 512(c)(2).

xxv. *Id.* § 512(c)(3)(A)(iv).

xxvi. The DMCA provides requirements for proper notification of possible copyright infringements in 17 U.S.C. § 512(c)(3)(A).

xxvii. Section 512(f) of the DMCA establishes civil liability when someone materially misrepresents to an ISP that information posted is infringing. The statute states:

> Any person who knowingly materially misrepresents under this section—
>
> (1) that material or activity is infringing, or
>
> (2) that material or activity was removed or disabled by mistake or misidentification,
>
> shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

17 U.S.C. § 512(f). While explicit civil liability is assessed against those who make misrepresentations to the ISP, there is no mention of whether the ISP may be liable for bad faith takedowns of material that proves not to be infringing.

xxviii. There is no specific provision for monetary or injunctive relief in the E-Commerce Directive. It is unclear whether individual European countries would provide private causes of action to enforce the Directive.

xxix. Section 512(f) of the DMCA permits a content creator to recoup damages caused by wrongful takedowns. If the content creator proves that the takedown request was made using material misrepresentations, it will have a claim for

> damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

17 U.S.C. § 512(f). *See* LEE A. HOLLAAR, LEGAL PROTECTION OF DIGITAL INFORMATION, ch. III.B.3 (2002), *available at* http://digital-law-online.info/lpdi1.0/treatise34.html (last visited Apr. 29, 2005).

xxx. One commentator has stated that:

> the question arises whether Internet service providers are liable for infringing material posted by users on their server. Infringing material could be for example, defamatory material, material in breach of copyright, material breaching criminal law (e.g. communications relating to criminal activities such as drug dealing; statements inciting racial hatred, child pornographic material). This involves problematic issues as to the enforcement of public law regulation against obscenity, the expression of racial hatred[,] etc.

Julia Hörnle, *The European Union Takes Initiative in the Field of E-Commerce*, J. INFO. L. & TECH, pt. 3.9 (Issue Three) (2000), *available at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/hornle.