Click Here for Lawsuit - Trespass to Chattels in Cyberspace

David M. Fritch

Follow this and additional works at: https://scholarship.law.ufl.edu/jtlp

Recommended Citation
Available at: https://scholarship.law.ufl.edu/jtlp/vol9/iss1/3

This Article is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in Journal of Technology Law & Policy by an authorized editor of UF Law Scholarship Repository. For more information, please contact kaleita@law.ufl.edu.
CLICK HERE FOR LAWSUIT — TRESPASS TO CHATTELS IN CYBERSPACE

David M. Fritch*

I. INTRODUCTION ............................................. 32

II. THE TRESPASS TO CHATTELS DOCTRINE .................. 35
   A. The Law of Trespass .................................... 36
   B. Trespass and the Internet — The Current
      Legal Landscape ....................................... 40
      1. eBay, Inc. v. Bidder's Edge, Inc. ..................... 40
      2. Ticketmaster Corp. v. Tickets.com, Inc. .............. 43

III. COMMONLY USED OBJECTIONS TO USING
     TRESPASS LAW ON THE INTERNET ....................... 44
   A. Applying Trespass Doctrine to Cyberspace Will Not
      Destroy the Internet .................................. 45
      1. Voluntary Internet Standards Currently Provide for
         the Right of a Web Site's Owner to Limit Access to
         Their Site from Legitimate Search Engines .............. 46
      2. Placing Limitations on the Ability to Link to
         Web Sites Does Not Undermine the
         Nature of the Internet ................................ 47
   B. Extending Trespass Doctrine to Include Electronic
      Interference with Another's Property Does Not Create a
      Unique Property Right in Cyberspace .................... 50
   C. Damages in Cyber-Trespass Cases Are Sufficient to
      Support a Trespass to Chattels Claim .................... 53
      1. Even If They Are Difficult to Measure, Damages in
         Cyber-Trespass Are Sufficient to Support a
         Trespass Claim ......................................... 53
      2. Cyber-Trespasses Temporarily Deny a Web Site
         Owner Use of Some Portion of Their Site's
         Resources, Sufficient to Support a Claim for
         Trespass to Chattels .................................... 54

* J.D. Candidate, 2005, Villanova University School of Law; M.S., 1997, University of
Colorado; M.A., 1993, Fairleigh Dickinson University; B.S., 1990, Boston University. The author
would like to thank his wife, Jennifer, for her insightful comments and patience on earlier drafts.
I. INTRODUCTION

The Internet has come a long way from its humble beginnings as a set of technology and standards to enable the free sharing of ideas and work in the research community.¹ The web boom of the 1990s brought the Internet beyond the research labs and universities and into the commercial mainstream, delivering the World Wide Web to the masses.² Today, the Internet is unparalleled as the world’s largest repository of content, accessible to anyone with a computer and a browser.³ Extending far beyond its historical roots as an experimental research network, this vast store of accessible information has evolved into a global one-stop

¹ See Nick Donofrio, The Nature of Computing, Address before the TECHXNY Conference (June 25, 2002), in 17 EXECUTIVE SPEECHES 4, Feb. 1, 2003 (noting that development of Internet and related technologies has been more “evolution” than “revolution”), available at 2003 WL 15423422.

² See UNESCO, THE WORLD COMMUNICATION AND INFORMATION REPORT 1999-2000, at 158, (noting 1990s was the decade of Internet commercialization and expansion), available at www.unesco.org/webworld/wirerpt/vers-web.htm (last visited Mar. 18, 2004). The move towards privatization of the Internet, however, has been occurring since the late 1970s when DARPA began to involve the outside research community in decision making for ARPANET (the precursor to the modern Internet) standards until this standard-making process was taken over by the private sector entirely in the mid 1980s. Id. at 159 (noting evolution of Internet from research tool to commercial network).

³ See Donofrio, supra note 1, at 11 (noting Internet’s evolution and growth). The common interfaces that interlinked computers and networks to form the Internet continue to expand to new devices, bringing society closer to “anywhere-anytime” access to this vast repository of information. Id. at 8.
information resource and communications network serving a host of public, private, and commercial interests.4

While the broad consumer impact of the Internet has garnered much of the attention for the Web's expansive promise, the compilation of information and the underlying technology to deliver it to the masses is not free. The cost of "anytime-anywhere" access to information is generally borne by companies investing in an online business model, with the need for a return on that investment. As one high-technology executive noted:

Sure, there are a ton of benefits for consumers and end users. But wristwatch stock trading and downloadable movies don't happen without a decision by an enterprise to create an infrastructure that enables those kinds of applications . . . that manages all those transactions . . . that keeps data flowing at ultra high speeds.5

This level of investment in generating and compiling enormous quantities of valuable information, coupled with the ability to make this information instantly accessible and easily replicable to web site visitors can lead to a "free rider" problem. The same technology that places the information within easy reach of customers makes it easily accessible, and replicable, to less desirable parties as well. Competitors can easily gather and use a web site's information for their own purposes — without incurring the costs of compiling and formatting the information firsthand.6


5. Donofrio, supra note 1, at 9.

6. "One need only to look at the Web to see how easy it has become to collect and copy information of any type." Blanke, supra note 4, at 647. For example, in Pollstar v. Gigmania, Ltd., the plaintiffs were engaged in compiling information regarding upcoming concerts, which it used to provide music business professionals with an accurate and reliable source of industry and concert information. See Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974, 976 (E.D. Cal. 2000) ("Pollstar alleges that it created and developed up-to-the-day time sensitive concert information that was published daily on its web site."); see also Pollstar, About Pollstar, available at www.pollstar.com/about_pollstar.pl (last visited Mar. 18, 2004). The defendant regularly accessed the plaintiff's web site, and copied the concert information onto its own competing web site. See Pollstar, 170 F. Supp. 2d at 976 (alleging Gigmania misappropriated Pollstar's information by copying and reusing information on its competing web site). The plaintiff claimed the value of this
Web technology, by its nature, allows one to easily piggyback on information compiled and located on another's web site. Using automated search robots or spiders, programmed to search the pages of a target web site, a person can easily search for and identify desired information across a variety of sites. Once located, the desired information can be copied over or linked to the originating web site and repurposed for the second site's use. While this sharing and interlinking of data between web sites is common practice on the Internet, it presents a unique problem by allowing the owner of one web site to easily appropriate the property of another site (for example, processing power, bandwidth, memory, etc.) to procure otherwise valuable information and further its own commercial aims.

This Article suggests that broader judicial recognition of traditional property rights for web sites would allow site owners to rely on historical standards to protect their data and give them the control over their web-based assets that is needed to facilitate a variety of business models and to continue to fuel the Internet's growth. Part II of this Article describes the information, namely the accuracy and time sensitivity of the data they compiled, was misappropriated by the defendant, and this "free riding" on their efforts reduced their incentive to collect and publish this information. Id. at 977 (alleging Pollstar was damaged by Gigmania's misuse of information posted on their web site).

7. See, e.g., Register.com v. Verio, 126 F. Supp. 2d 238, 242 (S.D.N.Y. 2000). The defendant in Register.com used an automated search robot to search a database of the plaintiff's customer information to generate leads for the defendant's services which were in direct competition with the plaintiff's services. Id. at 244-45.

8. See, e.g., Ticketmaster v. Tickets.com, 2003 WL 21406289, at *3, (C.D. Cal. 2003). Tickets.com, the defendant in Ticketmaster, employed an automated search robot to search the Ticketmaster site for desired event information, and then copied that information over to their own web site. Id. Tickets.com also provided direct links to the relevant event page on the Ticketmaster site from the Tickets.com site. Id. Another common complaint about "deep linking," or linking to a page on a web site other than the front page, is that the practice disrupts revenues for ad-supported web sites. See Farhad Manjoo, Site Barks About Deep Link, WIRED NEWS (May 1, 2002), at www.wired.com/news/politics/0,1283,52213,00.html; see id. commentary (Mar. 2, 2001), n.6. By connecting visitors directly to pages deep within a target site, these links allow a viewer to avoid advertising located on the main page — which can result in loss of advertising revenue to the targeted site. See id.; see also Pollstar, 170 F. Supp. 2d at 976 (bringing claim of common law misappropriation for concert data copied off plaintiff's web site and posted on defendant's site); Ticketmaster, 2003 WL 21406289, at *5 (noting claim of lost advertising revenue from deep linking).

9. See, e.g, eBay v. Bidder's Edge, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000) (noting that web sites are personal property and unauthorized use of automated spiders to search another's web site constitutes use of some portion of another's personal property). Unauthorized use of another's personal property is not a property right that is recognized under the law. Id. at 1071 (finding trespass to chattels from unauthorized web site searches).
trespass to chattels doctrine, as per the Restatement, and how it has begun to find its place in Internet law. Part III critiques the main issues raised in applying the trespass to chattels doctrine to unwanted electronic intrusions in cyberspace. Part IV concludes that the traditional principles of property law are both applicable and necessary, even in cyberspace.

II. THE TRESPASS TO CHATTELS DOCTRINE

Application of property law, with its ancient roots, to something as recently evolved as the Internet raises questions about the use of such antiquated laws in cyberspace. In spite of its "virtual" nature, the Internet readily lends itself to parallels with real property. Like real property, Internet sites are "fixed" in a cyberspace location. They are identified by an address, have definable borders and are capable of being exclusively controlled. Courts have also recognized these similarities by applying property law to cyberspace in upholding a registrant's property right in an Internet domain name, enabling claims of conversion for web sites, and

10. For a further discussion of the trespass to chattels doctrine, see infra text accompanying notes 13–62.
11. For a further discussion of criticisms levied against the cyber-trespass theory, see infra text accompanying notes 63–144.
12. For a further discussion of the applicability of trespass to chattels doctrine in cyberspace, see infra text accompanying notes 145–53.
13. See Richard Warner, Border Disputes: Trespass to Chattels on the Internet, 47 VILL. L. REV. 117, 120 (2002) ("applying the doctrine [of trespass to chattels] to the Internet carries the danger that courts will invoke a traditional, and possibly inappropriate, property right in ways that interfere with the Internet's life-blood.").
14. See Caffarelli, supra note 4, ¶ 9. The jargon of web sites, such as navigating the web, finding specific addresses, etc. all reflect the reality of the Internet as a form of property. Id. (noting parallels between real property and cyberspace).
15. See Richard A. Epstein, Centennial Tribute Essay: Cybertrespass, 70 U. CHI. L. REV. 73, 83 (2003). The early law distinguished personal property (chattels) from real property by whether the item was or was not movable. Id. Given the fixed nature of a web site and its cyberspace location, the rules of real property often provide a better fit. Id.
16. See Caffarelli, supra note 4, ¶¶ 22-25 (identifying cyberspace as property). The Ninth Circuit identified a three-part test to determine whether a property right exists. See G.S. Rasmussen & Assocs. v. Kalitta Flying Serv., 958 F.2d 896, 902-03 (9th Cir. 1992). For a property right to exist (1) there must be an interest capable of precise definition, (2) the interest in question must be capable of exclusive possession or control, and (3) the owner must have a legitimate claim to exclusivity. Id. Web sites meet all three of these criteria allowing them to be regarded as property, and therefore subject to the exercise of property rights. See Caffarelli, supra note 4, ¶¶ 22–23 (applying Rasmussen test to cyberspace).
17. See Kremen v. Cohen, 2003 WL 21715318, at *6, (9th Cir. 2003) (holding Internet domain name a form of intangible property, providing the basis for conversion claim against
enabling owners of web sites to bring claims of trespass to prevent unauthorized access to their site. 19

A. The Law of Trespass

Under the Restatement (Second) of Torts, trespass to chattels is defined as “intentionally dispossessing another of chattel or using or intermeddling with a chattel in the possession of another.” 20 Unlike trespass to land, where even harmless intrusions can impose liability, 21 liability under trespass to chattels requires that the trespassing party impair the quality or condition of the chattel or dispossess the possessor of their chattel. 22

In order to constitute a trespass, the intrusion must be one that is not permitted by the owner. 23 While web site owners may provide direct notice to an alleged trespasser that their intrusions are not permitted in an attempt to stop unwanted intrusions before bringing their claims to court, 24 such

---

19. See eBay, 100 F. Supp. 2d at 1067 (holding owners of web sites have right to exclude unwanted traffic).

One who intentionally enters land in the possession of another is subject to liability to the possessor for a trespass, although his presence on the land causes no harm to the land, its possessor, or to any thing or person in whose security the possessor has a legally protected interest.

Id.

22. RESTATEMENT (SECOND) OF TORTS § 218 (1965). “The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel.” Id. cmt. e. “The deprivation of use, not amounting to a dispossession, necessary to render the actor liable for his use or other intermeddling with the chattel of another without the other’s consent must be for a time so substantial that it is possible to estimate the loss caused thereby.” Id. cmt. i.
23. The term “trespass” is limited to intentional interferences. RESTATEMENT (SECOND) OF TORTS § 217 cmt. b (1965). It is necessary that the trespasser know that his actions are intermeddling with the possessory interest of another. Id. cmt. c.
24. For example, in eBay, eBay notified Bidder’s Edge verbally and in writing that their actions were unauthorized prior to bringing suit. See eBay v. Bidder’s Edge, 100 F. Supp. 2d 1058, 1062 (N.D. Cal. 2000). Bidder’s Edge continued to crawl eBay’s site, actively evading eBay’s efforts to block their activities using “rotating” proxy servers. Id. at 1063-64.
direct notification may not be necessary. The question of what is and what is not permissible access to a web site is generally answered by that site's terms of use (usually found on the site itself). Access to a web site, with knowledge or presumptive knowledge of these terms, constitutes an enforceable contract between the site owner and the visitor, with acceptance of the site owner's terms. This allows site owners to place limitations on the consent granted to site visitors, defined by the specified terms for allowable access and permissible use of data found on the site.

25. Under the Restatement (Second) of Torts, if a web site were deemed a public utility or common carrier (like phone companies, gas and electric companies, innkeepers, etc.), it would be required to permit any use of its chattels that is reasonably necessary to the enjoyment of their site. See Restatement (Second) of Torts § 259 (1965). Web sites, however, are not deemed a public utility, even though they open themselves to public access. See Island Online, Inc. v. Network Solutions, Inc., 119 F. Supp. 2d 289, 306-07 (E.D.N.Y. 2000) (“the Internet is, by no stretch of the imagination, a traditional and exclusive public function”); Register.com v. Verio, 126 F. Supp. 2d 247 (S.D.N.Y. 2000) (denying the defendant privilege to access plaintiff’s web site on grounds of web sites being a public utility).

26. See Caffarelli, supra note 4, at *47 (“once a [web site] creator established a set of guidelines, the consent or permission granted by the rules would limit a visitor’s freedom to interact or ‘intermeddle’ with the site”); see also eBay, 100 F. Supp. 2d at 1068 (finding ability to crawl public web site governed by the terms of the site owner’s license agreement).

27. See Ticketmaster Corp. v. Tickets.com, Inc., 2003 WL 21406289, at *2 (C.D. Cal. 2003) (holding that contract is formed by proceeding into the interior web pages after knowledge, or presumptive knowledge, of the conditions accepted in doing so). Web sites, and their servers, are private property to which the public is granted conditional access. See eBay, 100 F. Supp. 2d at 1070. The terms of this access are at the discretion of the site owner. Id. Web site owners may, however, be held to make their license terms governing the use of the site, and information on the site, prominent to site visitors in order to claim presumptive knowledge. See Ticketmaster, 2003 WL 21406289, at *2 (finding that warning that proceeding further binds web site visitor to conditions of use when placement of warning “could not be missed”); see also Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002) (finding no mutual assent when notice of existence of license terms governing software use was visible to Internet users only by scrolling down the screen).

28. Rather than “shrink wrap” licenses applied to the outside packaging on software, the Pollstar court termed web site licenses “browse wrap” licenses, which are part of the web site itself, asking for visitors to assent to their terms when visiting the web site. See Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974, 981 (E.D. Cal. 2000). In Pollstar, the license agreement limiting use of any information gathered from the plaintiff's web site was not set forth on the home page, but rather on a different web page, hyperlinked to the home page. Id. Visitors to the plaintiff’s web site were alerted that “use is subject to license agreement” by way of notice provided in small gray print on gray background. Id. The text linking to the license agreement was not underlined, as common Internet practice to show an active link mandates. Id. The Pollstar court raised the concern that many users presumably are not aware the license agreement is linked to the home page. Id. While the Pollstar court agreed with the defendant that visitors to the plaintiff’s web site were not immediately confronted with the notice of the license agreement, the Pollstar court did not find this made the license agreement terms invalid and unenforceable. Pollstar, 170 F. Supp. 2d at 982. "Taking into consideration the examples provided by the Seventh Circuit — showing that people
Visitors who exceed the scope of the consent granted to use a web site’s resources are deemed to be trespassing. 29

Under early common law, trespass claims were limited to physical intrusions or touching of another’s land or chattels. 30 Modern law, however, recognizes indirect touching or entry as well as intangible intrusions as sufficient to support a trespass to chattels claim. 31 In a landmark case expanding trespass doctrine to the information age, a California Court of Appeals in Thrifty-Tel, Inc. v. Bezenek 32 found that unwelcome electronic signals transmitted over the plaintiff’s telephone network were a sufficiently tangible intrusion to support a claim of trespass. 33 Noting that the Restatement includes “intermeddling” in its definition of trespass to chattels, the Thrifty-Tel court found that unwanted
electronic transmissions over a communications network constituted intermeddling with another’s chattels.\textsuperscript{34}

The plaintiff in \textit{Thrifty-Tel} was a small telephone company whose limited network was overburdened by the defendant’s unauthorized transmissions, causing some subscribers to be denied access to their phone lines.\textsuperscript{35} By denying use of the plaintiff’s network to paying customers, the defendant’s actions deprived the plaintiff of the use of their property for a substantial time, thus meeting the Restatement’s requirement of an actionable trespass.\textsuperscript{36} Linking to and searching of web sites, however, often involve the use of only a small portion of a web site’s resources. These activities rarely, if ever, consume sufficient site resources to block legitimate web traffic or prevent an owner from deriving the benefits of their web site.\textsuperscript{37} This distinction raises questions as to whether such trespasses are actionable.\textsuperscript{38}
B. Trespass and the Internet — The Current Legal Landscape

Two recent California cases demonstrate the issues surrounding the applicability of the emerging doctrine of cyber-trespass and how similar facts can lead to divergent results. 39

1. eBay, Inc. v. Bidder’s Edge, Inc. 40

In eBay, the defendant, Bidder’s Edge, operated an online auction aggregation web site that listed information on items being auctioned from more than one hundred online auction sites. 41 The plaintiff, eBay, operated the largest consumer-to-consumer auction web site on the Internet. 42 Given eBay’s size, it was important for Bidder’s Edge to include data on eBay’s auctions on their site. 43 Bidder’s Edge used an automated search robot to gather information for its site by searching targeted auction sites for auction data and copying the relevant information over to the Bidder’s Edge web site. 44 When the parties failed to reach an agreement on license terms that would allow Bidder’s Edge to continue conducting searches of

39. Other cases have also dealt with the question of cyber-trespass. See, e.g., Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (finding company’s automated searching of competitor’s web site to gather marketing leads actionable trespass); America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998) (holding unsolicited sending of bulk e-mail actionable trespass to chattels); CompuServe, Inc. v. Cyber Promotions, Inc., 963 F. Supp. 1015 (S.D. Ohio 1997) (finding bulk e-mail diminished value of plaintiff’s equipment sufficient to support trespass to chattels claim); cf. Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32 (Cal. 2003) (holding unwanted e-mails failed to cause sufficient injury to plaintiff’s computer systems for actionable trespass to chattels claim).

40. 100 F. Supp. 2d 1058.

41. Id. In March 2000, when the eBay suit was decided, the Bidder’s Edge web site listed information on more than 5 million items being auctioned on more than 100 auction sites, as well as additional auction-related services and information. Id. at 1061. Bidder’s Edge maintained a searchable database compiled by automated queries of online auction sites which allowed their users to search for a given item across multiple auction sites. Id. at 1062.

42. Id. At the time of the suit, eBay had over 7 million registered users, with over 400,000 new items added to the site every day. Id. at 1060. Users on eBay performed, on average, 10 million searches per day, placing 600 bids per minute on almost 3 million posted items. Id. eBay bills themselves as “the World’s Online Marketplace™,” noting that eBay is “the most popular shopping destination on the Internet.” eBay, Company Overview, n.6, at http://pages.ebay.com/community/abouteBay/overview/index.html.

43. At the time of the lawsuit, approximately 69% of the auction items listed on the Bidder’s Edge site were from eBay. See eBay, 100 F. Supp. 2d at 1063. Bidder’s Edge estimated that it could lose one-third of its users if it could not include the eBay auctions in its listings. See id.

44. Id. at 1061. By aggregating the auction information in their own database, visitors to the Bidder’s Edge web site were able to search a single database, which compared auction listings from more than one hundred auction sites, without having to search each site individually. Id. at 1062.
eBay’s site, eBay notified Bidder’s Edge that its activities were a violation of its license agreement and attempted to electronically block its searches.\textsuperscript{45} When these efforts failed to prevent Bidder’s Edge from accessing their site, eBay went to court seeking an injunction against Bidder’s Edge to stop it from using its automated search robot to gather auction information from the eBay web site.\textsuperscript{46} Based on a claim of trespass to chattels, eBay successfully obtained a permanent injunction from a federal court in the Northern District of California, stopping Bidder’s Edge’s online searches of the eBay web site.\textsuperscript{47}

While eBay alleged calculable monetary damages, the eBay court found no evidence of specific incremental damages from the defendant’s

\textsuperscript{45} Id. at 1062. The version of eBay’s user agreement in force at the time the suit was decided specifically prohibited the use of “any robot, spider, other automatic device, or manual process to monitor or copy our web pages or the content contained herein without our prior expressed written permission.” Id. at 1060. It was not clear to the eBay court, if the then-current version of eBay’s user agreement was in effect when Bidder’s Edge began searching the eBay site. Id. The documented communications between the parties, however, left no question that Bidder’s Edge had knowledge that its searches of eBay’s web site were unwelcome. Id. at 1062. eBay attempted to identify unwelcome robotic activity on its site by monitoring the number of incoming requests from each particular IP address (a unique identifier assigned to each computer to enable it to communicate over the Internet), and blocking further requests from specific IP addresses it believed were conducting unauthorized activities on its site. eBay, 100 F. Supp. 2d at 1061. Blocking queries from individual IP addresses, however, is not always successful. Id. Outgoing requests, like the searches from Bidder’s Edge, can be routed through proxy servers so that they appear to the incoming site as originating from that proxy server (with a different IP address). Id. Information requests routed through these proxy servers are not easily traceable back to the originating IP address, and are often used to circumvent any attempt to block access from a particular address. Id. While eBay had blocked a total of 169 IP addresses it believed Bidder’s Edge was using to query their site, Bidder’s Edge employed “rotating proxy servers” to evade eBay’s blocks. Id. at 1062-63. This practice leads to what the eBay court termed a game of “hide-and-seek,” which can be potentially counterproductive since it runs a substantial risk of blocking legitimate and desirable users (who use a particular proxy server) from accessing the site. Id. at 1061.

\textsuperscript{46} Id. at 1060. The main dispute between eBay and Bidder’s Edge was the method that Bidder’s Edge used to search eBay’s site. Id. at 1062. eBay wanted Bidder’s Edge to conduct searches of its system only when a user queried the Bidder’s Edge system. Id. Bidder’s Edge wanted to crawl eBay’s site recursively to compile its own database. Id. The method used by Bidder’s Edge allowed it to better track the auctions and automatically update its users when activity occurred in a particular auction. eBay, 100 F. Supp. 2d at 1062. This method, however, creates an increased load on eBay’s systems from the searches of Bidder’s Edge. Id. The injunction sought by eBay, however, was not limited to restricting how Bidder’s Edge could take data from eBay’s site. Id. at 1063.

\textsuperscript{47} Id. at 1073. The eBay court order did not, however, preclude Bidder’s Edge from using information obtained from eBay’s site “other than by automated query program, robot, web crawler, or similar device.” Id. at 1073.
activities. The eBay court did, however, find that while the defendant’s activities represented a small load on eBay’s web site resources, the cumulative effect of Bidder’s Edge and other parties like it, if given unchecked access to eBay’s system, could create a debilitating load on eBay’s servers sufficient to support a claim of trespass. While the eBay court found this possibility of irreparable harm to eBay’s system sufficient to grant an injunction on the merits of eBay’s trespass claim, it also presented a more compelling reason for its ruling.

The eBay court found computer trespass more akin to trespass to property than trespass to chattels since even ongoing trespass may never amount to a conversion. The eBay court determined that if eBay was operating a traditional auction house, it would have the right to limit access to potential bidders and close its doors to competitors. Noting that the right to exclude others is a fundamental right of a property owner, the eBay court found the unwanted web searches an ongoing violation of that

48. eBay, 100 F. Supp. 2d at 1063. eBay alleged damages between $45,323 and $61,804 from the activities of Bidder’s Edge. Id. The eBay court found these calculations flawed, since they assumed maximum usage of eBay’s resources over the entire ten month period in question and attributed a pro rata share of eBay’s total expenditure to the activities of Bidder’s Edge, rather than giving a precise calculation of the incremental cost to eBay from the activities of Bidder’s Edge. Id.

49. Id. at 1066. The eBay court found that denial of preliminary injunctive relief for eBay would “present a strong likelihood of irreparable harm.” Id. Reasoning that, while one crawler may use only one percent of eBay’s resources, if hundreds of other companies used similar crawlers on eBay’s site, eBay would be “brought to its knees by what would then be a debilitating load.” Id. at 1066 n.14.

50. Id. at 1066-67 (finding actionable trespass based on right to exclude unwanted web site traffic).

51. Id. at 1067 (finding defendant’s activities a violation of plaintiff’s fundamental property rights).

52. Id. (noting problems of permitting unauthorized web site access).

If eBay were a brick and mortar auction house with limited seating capacity, eBay would appear to be entitled to reserve those seats for potential bidders, to refuse entrance to individuals (or robots) with no intention of bidding on any of the items, and to seek preliminary injunctive relief against noncustomer trespassers. Id.

53. See eBay, 100 F. Supp. 2d at 1066-67. The eBay court characterized the right to exclude others as “one of the most essential sticks in the bundle of rights that are commonly characterized as property.” Id. (quoting Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979)).
fundamental right, concluding the appropriate remedy for ongoing cyber-trespass is issuance of a preliminary injunction.  

2. Ticketmaster Corp. v. Tickets.com, Inc.  

In Ticketmaster, the plaintiff operated an online ticket sales site that offered information to the public on events for which it sold tickets, listing the event’s date, time, and ticket price, as well as information on ordering tickets online. Tickets.com was a direct competitor to Ticketmaster who also provided event information to the public via its web site, whether it sold tickets to the event or not. For events where Ticketmaster was the exclusive seller of tickets, Tickets.com created “deep links” to send visitors directly to the corresponding event pages on Ticketmaster’s web site. Tickets.com created these “deep links” by using an automated spider to search Ticketmaster’s web site and copy the desired factual information about the event from Ticketmaster’s site onto the Tickets.com web site.
(ticket price, date, time, URL, etc.) thus creating the relevant “deep link” to the Ticketmaster site.\textsuperscript{59}

Ticketmaster brought suit in the Central District of California alleging, among other things, trespass to chattels from Tickets.com’s unauthorized use of spiders to search and copy information from its web site, as well as providing unauthorized deep links to its site, allowing visitors to access information on its site and bypass its main page (and associated advertising).\textsuperscript{60} In evaluating the trespass claim, the \textit{Ticketmaster} court noted the weight of other district cases found the mere invasion or unauthorized use of a portion of a web site by a spider is a trespass, even without a showing of direct harm or tangible interference with the invaded computer.\textsuperscript{61} The \textit{Ticketmaster} court disagreed with the other district court findings and refused to find a tort claim without evidence of tangible tort-like damages to the affected web site.\textsuperscript{62}

\section*{III. Commonly Used Objections to Using Trespass Law on the Internet}

While courts have generally appeared willing to apply the trespass to chattels doctrine to the Internet, many legal scholars have criticized the application of such an ancient legal doctrine to the new world of

\textsuperscript{59} See id. Tickets.com’s electronic spider temporarily loaded the desired event information into the Random Access Memory (RAM) of Ticketmaster’s computers for a period of from 10-15 seconds. \textit{Id.} at 2.

\textsuperscript{60} See \textit{Ticketmaster}, 2003 WL 21406289, at *2. Ticketmaster also brought suit on a contract basis, alleging Tickets.com’s activities violated Ticketmaster’s license agreement. \textit{Id.}

\textsuperscript{61} \textit{Id.} at *3 (noting numerous published and unpublished district court cases discussing chattel theory).

These cases tend to support the proposition that ‘mere invasion or use of a portion of the web site by a spider is a trespass (leading at least to nominal damages), and that there need not be an independent showing of direct harm either to the chattel (unlikely in the case of a spider) or tangible interference with the use of the computer being invaded.

\textit{Id.}

\textsuperscript{62} \textit{Id.} (“requiring some tangible interference with the use or operation of the computer being invaded by the spider.”). The \textit{Ticketmaster} court “respectfully disagree[d] with other district courts’ finding that mere use of a spider to enter a [publicly] available web site to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels.” \textit{Id.} The \textit{Ticketmaster} court characterized Ticketmaster’s trespass claim in this context as attempting “to apply a medieval common law concept in an entirely new situation which should be disposed of by modern law designed to protect intellectual property interests.” \textit{Id.}
The objectors to the application of chattels doctrine to cyberspace criticize it on grounds of the unique nature of the Internet and the antiquity of the trespass doctrine.

A. Applying Trespass Doctrine to Cyberspace Will Not Destroy the Internet

Critics of the chattels theory fear that allowing web site owners to exert control over who can access a web site and the means by which they can access that web site will have "disastrous implications for basic types of behavior fundamental to the [I]nternet." Since open access to information on the Web has been, and continues to be, the lifeblood of the Internet, some fear the application of antiquated notions of property and trespass may threaten the critical interests of cyberspace. One of the most cited fears is that trespass doctrine, if applied to cyberspace, threatens the legality of the search engines that make finding useful information in the vast repository of the Internet feasible. What this argument fails to take into account, however, is that Internet standards and technology have already granted web site owners the type of power needed to control

63. Id. (recognizing legal scholars' criticisms of cyber-trespass claims). In spite of the weight of case law supporting the proposition of trespass to chattels in cases like this, the Ticketmaster court noted there is a good deal of scholarly work criticizing the extension of the trespass to chattels doctrine to an Internet context. Id.; see, e.g., Quilter, supra note 38, at 441 (finding trespass doctrine ill-suited to cyberspace); Merrell, supra note 30, at 675 ("Applying trespass to chattels to the Internet is like driving a horse and buggy on the information superhighway.").

64. Many scholars characterize this as a "quick fix" by courts to troublesome Internet issues, without recognizing the inherent shortcomings of the application of an ancient legal doctrine to cyberspace. See, e.g., Quilter, supra note 38, at 435 (characterizing trespass to chattels on the Internet as a new form of property protection that is beyond a court's powers to create).


66. See Warner, supra note 13, at 119. The Internet is a modern phenomena while trespass doctrine evolved in a very different economic and technological setting. See id. This leaves questions as to whether the trespass doctrine can properly balance the interests of businesses and users on the Internet. See id.

67. See Lemley Brief at 8, eBay (No. 00-15995) (calling search engines "one of the fundamental building blocks of the Internet."). Since search engines generally rely on the same spider technology used by the defendant in eBay, Lemley and twenty-seven other law professors, in their amicus curiae brief expressed fear that the eBay court's decision would make the functioning of search engines an illegal activity. Id. (noting similarity of search engine technology and spiders used by defendant in eBay).
access to their web sites.\textsuperscript{68} The law of trespass simply affirms and gives a legal framework to these rights.

1. Voluntary Internet Standards Currently Provide for the Right of a Web Site's Owner to Limit Access to Their Site from Legitimate Search Engines

At the most basic level, the Internet functions as a series of interconnected networks, linked together by largely voluntary protocols and standards.\textsuperscript{69} One of these voluntary standards is called the "Robots Exclusion Protocol" which enables a web site owner to direct an automated search robot to bypass all or part of a web site, provided the search robot employed complies with this standard.\textsuperscript{70} In spite of the informal and voluntary nature of the standard, major search engines like Yahoo, Google, Excite, MSN and others adhere to the standard, providing site owners the ability to opt out of Internet search engines.\textsuperscript{71}

\textsuperscript{68} For a discussion of the application of the voluntary Robot Exclusion Standard to direct search engines to avoid searching all or part of a site, see infra notes 70 & 71. For a discussion of other technological solutions to avoid unwanted web site links and automated database searches, see infra notes 78 & 79.


\textsuperscript{70} \textit{See} Web Robots Pages, \textit{A Standard for Robot Exclusion}, \textit{available at \url{http://www.robotstxt.org/wc/norobots.html}} (last visited Mar. 2, 2004). This standard allows a web site owner to indicate to visiting robots that the site (or part of the site) should not be visited. \textit{Id.}

[The Robot Exclusion Standard] is not an official standard backed by a standards body, or owned by any commercial organization. It is not enforced by anybody, and there [are] no guarantee[s] that all current and future robots will use it. Consider it a common facility the majority of robot authors offer the WWW community to protect WWW server[s] against unwanted accesses by their robots. \textit{Id.}

\textsuperscript{71} \textit{See} eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1063 (N.D. Cal. 2000) (noting "[i]t appears that major Internet search engines, such as Yahoo!, Google, Excite and AltaVista, respect the Robot Exclusion Standard"). \textit{See, e.g.,} Google.com, \textit{Google Information for Webmasters} (providing direction to webmasters for excluding their site from Google’s searches using Robot Exclusion Protocol), \textit{available at \url{http://www.google.com/webmasters/3.html}} (last visited Mar. 2, 2004). "[B]efore crawling a site/directory, [the MSN search robot,] MSNBOT[,] will look at the first line of the robots.txt file. If it finds the User-Agent 'MSNBOT,' MSNBOT will honor the request and will not crawl the site/directory." MSN, \textit{The MSN Search Prototype Web Crawler — Frequently Asked Questions}, \textit{available at \url{http://search.msn.com/msnbot.htm}} (last
While the ongoing functionality of Internet search engines is held out as an overwhelming public interest justifying not giving site owners the right to control access to their sites, these search functions already voluntarily yield to the wishes of site owners. In spite of the view held by critics of cyber-trespass, who see cases like eBay and Ticketron as attempts from large companies to hamper the flow of information on the Internet to their benefit, the egalitarian auspices of encouraging the free flow of information do not translate as readily to granting unlimited gratuitous license to commercial companies who want to gather another web site’s information, repackage it, and then redistribute it for profit.

2. Placing Limitations on the Ability to Link to Web Sites Does Not Undermine the Nature of the Internet

The basic means of “navigating” the Internet, whether moving between pages within a site, or moving seamlessly between web sites, relies on the web’s ability to interlink pages and information. While opponents of cyber-trespass laws cite their potential to hamper linking on the Internet, people more familiar with web site development know there are technical
solutions for those who wish to control access to their web sites. 76 Web site owners can password-protect their sites, install scripts to break deep links, 77 or employ schemes where computer-generated permission tokens are embedded in authorized links, blocking all unauthorized direct links, to control other sites' ability to link to their site. 78 Other sites use images with codes embedded in them that cannot be read by a machine, but must be re-entered by the user before proceeding with an information request to prevent automated programs from searching online databases. 79

All of these technology-based solutions offer web site owners a straightforward means of controlling access to their site, but at a price. These measures all add cost and complexity, both to web site owners and to legitimate users, by adding additional steps and hurdles between the user and the desired information in an attempt to filter out unauthorized uses while still permitting authorized access. 80 While critics of the chattels doctrine decry its potential impact on the free and robust exchange of information, 81 the ambiguity of potential legal recourse in this area forces


78. A name token is "a string composed of any combination of name characters." Techdictionary.com, Token, available at www.techdictionary.com (last visited Mar. 2, 2004). A URL token scheme dynamically creates the link address when a visitor clicks on an authorized link, embedding a randomly generated permission token into the URL link. Deacons, supra note 76. The generation of these tokens can be done on a timed basis, "so that the permission token changes every hour or every day." Id. A link created using an expired token "will not let a visitor get to the sought-after page, or [will] alternatively bump the visitor to the gateway page." Id.

79. For example, visitors seeking to search the WHOIS database must first enter a code, embedded in a displayed image, used to prevent automated programs from requesting information from the database. See, e.g., Network Solutions, Inc., WHOIS Search, available at http://www.networksolutions.com/en_US/whois/index.jhtml (last visited Mar. 2, 2004). Users entering a domain name to search for on this page are directed to a screening page which asks visitors to enter an alphanumeric code displayed on the screen embedded in an image before continuing with the search. Id. The WHOIS database is the same database of domain name information at issue in Register.com, where the plaintiff sought an injunction to prevent the defendant from conducting automated searches of its database. See Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 241 (S.D.N.Y. 2000).

80. See infra note 79 (showing an example of the additional manual steps required for users seeking information from the WHOIS online database that resulted from the security measures employed to prevent unauthorized searches).

81. See Lemley Brief at 10, eBay (No. 00-15995) (claiming eBay court's decision threatens "free and robust exchange of information that has become the celebrated hallmark of the Internet.").
web site owners to employ countermeasures that increase the chances of legitimate, desirable users getting caught in efforts to screen for unwanted visitors, thus denying their legitimate access to the information they seek.82

For example, when eBay sought to prevent Bidder’s Edge from searching its web site, it began blocking traffic from Internet Protocol addresses it believed Bidder’s Edge used to search the eBay site.83 The tactic did little to dissuade Bidder’s Edge, since it began using rotating proxy servers to mask the identity of its traffic and evade these blocks; however, this resulted in eBay blocking 169 IP addresses during this time, thus denying all traffic to eBay’s site from those blocked IP addresses.84 Unfortunately, IP addresses are often shared resources, so blocking unwanted traffic from one IP address has the unintended result of blocking legitimate traffic from that same address as well.85 While Bidder’s Edge complained the injunction against it “restricts the openness that has made the Web such a powerful marketplace and so valuable to users,”86 they made no mention of the impact on legitimate users of eBay who were unfortunate enough to inadvertently share one of the 169 IP addresses used by Bidder’s Edge during this time who wished to legitimately access the eBay web site.87

82. Efforts to block traffic to web sites “can be easily circumvented and will seriously disrupt legitimate e-commerce and speech.” Stewart Baker, Prepared Statement of Mr. Stewart Baker General Counsel, U.S. Internet Service Provider Association, Committee on Senate Banking, Housing and Urban Affairs (transcript available in the Federal Document Clearing House, Inc.).


84. Id. at 1062-63. The eBay court noted the potentially counterproductive nature of the endless game of “hide-and-seek” played by web site owners and those attempting to circumvent attempts to block them as “run[ning] a substantial risk of blocking requests from legitimate, desirable users.” See id. at 1061.

85. See Baker, supra note 82. Part of the reason blocking traffic by IP address disrupts “a large number of lawful communications and legitimate commerce” is that many different web sites and users can share a single IP address. Id. The Internet is commonly populated by IP addresses that have been “contaminated, perhaps permanently, because they once hosted spammers thus causing those address blocks to be entombed into the memories of an unknown number of anti-spam filters not merely at the end user level but also deep in the routing infrastructure of the net.” Karl Auerbach, Is the Internet Dying?, CIRCLEID (Aug. 20, 2003) available at http://www.circleid.com/article/215_0_1_0_C/ (last visited Mar. 2, 2004).


87. See eBay, 100 F. Supp. 2d at 1062-63. Recent statistics show that 87% of all active domain names share their address with at least one other domain name and more than 66% of active domain names share their addresses with 50 or more additional domains. Baker, supra note 82 (citing Harvard Law School study).
B. Extending Trespass Doctrine to Include Electronic Interference with Another’s Property Does Not Create a Unique Property Right in Cyberspace

Notwithstanding the precedent established in Thrifty-Tel, critics of the chattels doctrine claim that contacting another’s equipment with electrons is insufficient to satisfy the physical contact needed for a trespass. Such an extension of trespass doctrine, it is claimed, leads to such “absurd results” as trespass to fax machines and unwanted phone calls. What this argument lacks, however, is the distinction of consent that typically governs each of these transactions. All of these nonphysical interactions are typically governed by the doctrine of implied consent that permits even unwelcome interactions until a party is told otherwise. Violation of this consent, even without a strictly physical intrusion, has consistently been held as grounds for the expansion of the trespass doctrine across a variety of mediums.

88. See Merrell, supra note 30, at 689 (citing claims of trespass by electrons “...too ethereal and metaphysical to justify a cause of action at law.”).

89. See id. “Such claims seem too tenuous to satisfy the physical contact element of an intentional tort like trespass to chattels.” Id. “If a chattel’s receipt of an electronic communication constitutes a trespass to that chattel, then not only are unsolicited telephone calls and faxes trespasses to chattel, but unwelcome radio waves and television signals also constitute a trespass to chattel every time the viewer inadvertently sees or hears the unwanted program.” Intel v. Hamidi, 1 Cal. Rptr. 3d 32, 46 (Cal. 2003).

90. See Epstein, supra note 15, at 85. Critics often argue that web site owners consented to the trespass by opening their site to millions of Internet users. Merrell, supra note 30, at 693. The argument follows that by having open access to a web site, it is reasonable to expect undesirable traffic to take up their site’s limited capacity. Id. Some critics believe this implied consent should be limitless and irrevocable, holding that “consent should be an allowable defense to chattels claim on the Internet, irrespective of attempts to negate that consent.” Id. at 694. The majority of courts have disagreed with this unlimited implied consent doctrine, allowing it to be expressly withdrawn, or governed by a site’s license agreement. See, e.g., eBay, 100 F. Supp. 2d at 1070 (holding visitor’s terms of use limited by license terms on web site, and by express notification from site’s owner); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000) (holding submitting of query to online database binds party to site’s terms of use).

91. See Epstein, supra note 15, at 85. “[S]ocial expectations make it clear that ordinary phone calls and faxes are not trespasses, any more so than routine entries into department stores.” Id. “[C]onsent is implied from the circumstances until the owner tells the entrant to stay off (if not on the premises) or leave (if he is).” Id.

92. For a discussion of the trespass doctrine applied to unwanted commercial mail, see infra text accompanying note 95. For a discussion of trespass doctrine applied to unwanted telemarketing calls and e-mails, see infra text accompanying note 100.
The U.S. Supreme Court has upheld actionable trespass claims based on unwanted mail violating an individual’s right to reject that mail. In *Rowan v. U.S. Post Office*, the U.S. Supreme Court expanded the traditional right of persons to bar peddlers and solicitors from their property by order or notice, therefore recognizing a person’s right to bar nonphysical intrusions in the form of unwanted mailings to their address. To hold differently, the Court held, would “license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering his home.”

Other nonphysical interactions have been subjected to similar restrictions. For example, unsolicited fax advertising is expressly prohibited under federal law. The Eighth Circuit upheld this prohibition in *Nixon, ex rel. v. American Blast Fax, Inc.*, where it allowed persons to expressly refuse to receive unsolicited faxes, and thus upheld the ability of the Federal Trade Commission to enforce criminal penalties on fax senders who persist in spite of a recipient’s refusal. Recent legislation also allows consumers to refuse unwanted commercial phone calls, and similar provisions are under consideration by Congress to prevent the

---

94. Id.
95. Id. at 737 (holding householder exclusive and final judge over what mail he or she will receive). The U.S. Supreme Court in *Rowan* found actionable trespass, even in the absence of physical damage or dispossession, based solely on the violation of a person’s prerogative “to be free from sights, sounds and tangible matter we do not want.” Id. at 736. The Court in *Rowan* deemed a mailer’s “right to communicate is circumscribed only by an affirmative act of the addressee giving notice that he wishes no further mailings from that mailer.” Id. at 737. While the addressees did not demonstrate any physical damage to their chattels, like the kind sought by critics of the chattels doctrine, the Court found that the unwanted mail violated the “wall” that a citizen may erect so that no one “may penetrate without his acquiescence,” providing sufficient damages to justify government intervention to prevent further intrusions. See id. at 738. While limiting receipt of unwanted mail clearly has the effect of impeding the free flow of ideas and communications, the *Rowan* Court found the right to communicate “must stop at the mailbox of an unreceptive addressee.” *Rowan*, 397 U.S. at 737.
96. Id. (upholding right of every householder to control unwanted mail).
98. 323 F.3d 649 (8th Cir. 2003).
99. See id. at 660 (holding restriction on unsolicited commercial fax advertisements “achieves a reasonable fit between the means it adopts and the ends it seeks to serve”).
transmission of unsolicited commercial e-mail. All of these restrictions recognize the applicability of traditional trespass doctrine to prohibit even nonphysical intrusions where the recipient has expressly withheld their consent.

100. See Federal Trade Commission, Telemarketing Sales Rule, 16 C.F.R. § 310 (2003) (effective Mar. 31, 2003). Under this rule, consumers may place their phone number on a centralized “do-not-call” list to stop calls from all companies within the FTC’s jurisdiction (subject to certain exemptions). Id. § 310.4(a) The rule also requires telemarketers to disclose the identity of the seller, transmit caller ID information, and also restricts allowable calling times. Id. § 310.4(a)(7)-(e)(2) Violations of this rule could entail fines on the telemarketer of up to $11,000 per call. See Federal Trade Commission, Calling All Telemarketers: Amendments to the FTC’s Telemarketing Sales Rule, FTC FACT FOR BUSINESS, at 2 (Mar. 2003), available at http://www.ftc.gov/bcp/conline/pubs/buspubs/calling.pdf (last visited Apr. 20, 2004). While there have been last-minute legal maneuvers to prevent the rule from going into effect, a do-not-call list containing over fifty million home and cell phone numbers was placed in service on October 1, 2003, pending appeal of lawsuits filed on behalf of the Direct Marketing Agency, and others. See Jane Larson & David Ho, Do-Not-Call List Goes Into Effect, but Uncertainty Remains, ARIZ. REPUBLIC, Sept. 30, 2003. This legislation spawned a high-profile legal battle waged by the American Teleservices Association, and other industry groups, on behalf of their member companies to block the implementation of the new rule claiming the list would devastate the industry and violate the First Amendment rights of telemarketers. See Associated Press, Telemarketers Sue Over Do-Not-Call List, FOXNEWS.COM (July 28, 2003), at http://www.foxnews.com/story/0,2933,93091,00.html. In spite of these claims, the home phone numbers of at least eleven DMA executives were found on the FTC’s do-not-call registry. See Jack Courant, Telemarketing Execs on Do-Not-Call List, HARTFORD COURANT, Oct. 1, 2003, at A1. Jack Mahadevia, a retired DMA Senior Vice President admitted to signing up to block unwanted phone calls, claiming “[t]here are so many calls I don’t want . . . they are disturbing my routine.” Id. Similar provisions are under congressional proposal to prohibit unsolicited commercial e-mails. See To Prevent Unsolicited Commercial Electronic Mail, H.R. 2214, 108th Cong. (2003) (proposing legislation permitting persons to opt out from unsolicited commercial e-mail and providing criminal penalties for parties who transmit these e-mails after recipient has opted out). Some states, like California, have already begun to take legislative action against unsolicited e-mail on their own. See, e.g., Reuters, Calif. Enacts Nation’s Toughest Anti-Spam Bill, USA TODAY, Sept. 25, 2003, at 3B (reporting recent California state law prohibiting unsolicited e-mail with fines up to $1 million per violation). Several states have statutes placing limitations on unsolicited commercial e-mails, such as requiring unsolicited commercial e-mail to be labeled at the beginning of the e-mail’s subject line with “ADV” and including opt-out instructions to the recipient which must be honored by the sender. See David E. Sorkin, Summary of State Spam Laws, available at http://www.spamlaws.com/state/summary.html (last visited Jan. 30, 2004). See also TEX. BUS. & COM. CODE ANN. § 46 (Vernon 2003) (providing criminal penalties for unsolicited commercial e-mail not properly labeled as advertising and requiring opt-out provision for future e-mail from sender).
C. Damages in Cyber-Trespass Cases Are Sufficient to Support a Trespass to Chattels Claim

The eBay court rejected eBay’s claims for specific monetary damages, yet it issued an injunction against Bidder’s Edge based on eBay’s trespass claim. Critics of the trespass doctrine claim that this and other similar precedents, create an “absolute property right, akin to trespass to land, but without the limiting doctrines and balances of real property law.” Under traditional tort law, in order to have an actionable claim for trespass to chattels, a trespasser must either dispossess the owner of their chattels or show some harm to the chattel resulting from the trespass.

1. Even If They Are Difficult to Measure, Damages in Cyber-Trespass Are Sufficient to Support a Trespass Claim

Damages in these types of claims require complex, and often unreliable, calculations of bandwidth factors, memory and processing power utilization, and foregone advertising revenues to demonstrate some quantifiable loss from a cyber-trespasser’s activities. The difficulty and

101. See eBay, Inc. v. Bidder’s Edge, Inc., 100 F. Supp. 2d 1058, 1065 (N.D. Cal. 2000) (holding eBay did not make “the required showing that this is the type of extraordinary case in which monetary damages may support equitable relief.”).

102. Quilter, supra note 38, at 441 (granting web site owners trespass to chattels remedy gives rights that do “not apply to any other communications medium (e.g., televisions and telephones).”).

103. See RESTATEMENT (SECOND) OF TORTS § 217 (1965) (permitting trespass claim for intentional dispossession of chattels); see also RESTATEMENT (SECOND) OF TORTS § 218 (1965) (permitting trespass claim for impairment of chattels’ quality or condition). “... While a harmless use or touching of personal property may be a technical trespass (see Rest.2d Torts, § 217), an interference (not amounting to dispossession) is not actionable,. . . without a showing of harm.” Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32, 40 (2003).

104. Various measures of damages have been proposed for these types of cyber-trespasses. For example, in eBay, the plaintiff attempted to estimate the impact of the defendant’s activities as part of the total load on its computer system (and collect a pro-rata portion of its total system costs for the portion of the system used by the defendant), as well as collect for reputational damage (from misleading postings of its information), and trademark dilution from the defendant’s actions. See eBay, 100 F. Supp. 2d at 1064-65. In Register.com, the plaintiff claimed lost processing power (citing a “rough estimate” of a 2.3% loss in system resources) from the defendant’s activities. See Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000). In Ticketmaster, the plaintiff claimed damages that included the value of the information taken by the defendant (the information was sold to other parties by the plaintiff) and the time and money expended in trying to frustrate the defendant’s attempts to access their site. See Ticketmaster Corp. v. Tickets.com, Inc., 2003 WL 21406289, at *3 (C.D. Cal. 2003). In deep linking cases, where a party provides a link to a target web site allowing readers to bypass the site’s front page, damages are often calculated as lost advertising revenues. See Manjoo, supra note 8. For example, the Dallas Morning News recently sent letters to site owners who linked directly to news articles on the paper’s web site, claiming that such links allow viewers to avoid the advertising on the home page. Id. Since
imprecise nature of tallying the amount of damages from a cyber-trespass helps to justify the decision to grant the injunctive relief often sought in these cases in lieu of monetary damages. The fact a plaintiff is willing to undertake expensive legal action in order to stop some conduct it believes is causing damage to its business provides sufficient evidence that there are significant damages involved, no matter how difficult it may be to quantify them.

2. Cyber-Trespasses Temporarily Deny a Web Site Owner Use of Some Portion of Their Site's Resources, Sufficient to Support a Claim for Trespass to Chattels

An actionable trespass to chattels does not always require a showing of physical damage to the chattel. Dispossessing another of their chattel or diminishing its value is also grounds for an actionable trespass. While most dispossession cases are serious enough interference to constitute a conversion, even seemingly minor dispossession, falling short of web banner advertising often charges on a per-view basis, each visitor who bypasses a page with online advertising constitutes a potential revenue loss to the site owner. See Thor Olavsrud, Tickets.com Wins One, INTERNETNEWS.COM (Aug. 15, 2000), at www.internetnews.com/ec-news/article.php/438011. For example, Ticketmaster.com received revenue from advertisers based on the number of hits on the page where the advertising is located. Id. In the case of Ticketmaster.com, at the time of the suit, both its home page and its interior pages carried advertising which generated revenue for Ticketmaster. Id. The difficulty in this information is calculating how many visitors are directed to these deep links that would have gone through the higher level pages and how many are purely incremental visitors to the target site. In many of these cases, however, the directing web site is still a competitor, even if it does direct incremental traffic to the target web site. See id. (noting Tickets.com remained a Ticketmaster competitor, regardless of incremental site traffic they directed to the Ticketmaster web site).

105. See Epstein, supra note 15, at 82 (“the very inability to estimate damages offers yet an additional reason to award injunctive relief”). The eBay court found that while there was “some uncertainty as to the precise level of possessory interference required to constitute an intermeddling, there does not appear to be any dispute [that] eBay can show the conduct of Bidder's Edge amounts to use of eBay's computer systems.” eBay, 100 F. Supp. 2d at 1070. In spite of eBay's inability to provide an acceptable calculation of damages attributable to the searches by Bidder's Edge, the eBay court found grounds to issue an injunction. Id. at 1072.

106. See Epstein, supra note 15, at 81 (“no plaintiff will sue to recover when the costs of litigation exceed the expected recovery of suit.”). While a web site may not be physically harmed in these cyber-trespass incidents, when a party takes information from a competitor's web site and potentially denies the owner of that site revenues, a reasonable business person could conclude these actions destroyed some of the web site's commercial, competitive value “thereby fulfilling the damage element of a trespass claim.” Caffarelli, supra note 4, ¶ 45.

107. RESTATEMENT (SECOND) OF TORTS § 218 (permitting actionable trespass claims for dispossessing persons of their chattels).

108. Id. § 218(a)-(b) (providing requirements for trespass to chattels claim).
interfering with another’s right of control, can support an actionable trespass claim.\textsuperscript{109}

The \textit{Ticketmaster} court rejected the plaintiff’s trespass claim, stating the elements required by the tort of trespass had not been met, specifically, tangible damage or dispossession of the chattel for a significant time.\textsuperscript{110}

While the \textit{Ticketmaster} court did not find it sufficient enough to be actionable, there was a dispossession element, no matter how minor, to Tickets.com’s activities.\textsuperscript{111} The spider used by Tickets.com temporarily loaded event information into the RAM of Ticketron’s computers for a period of ten to fifteen seconds while the spider extracted the desired information for transfer to the Tickets.com web site.\textsuperscript{112} When an unauthorized visitor uses a portion, no matter how small, of a web site’s resources, access to those resources is unavailable to the owner or other desirable visitors.\textsuperscript{113} This unauthorized and uncompensated use of

\begin{itemize}
  \item[109.] \textsc{Restatement (Second) of Torts} § 222 cmt. a (1965) ("[A] dispossession is always a trespass to the chattel, and subjects the actor to liability for at least nominal damages for the interference with the possession."). Even “taking another man’s hat by mistake and returning it within two minutes upon discovery of the mistake” is trespass sufficient to allow recovery for damages for the interference with the possession. \textit{Id.}
  \item[110.] See \textit{Ticketmaster Corp. v. Tickets.com, Inc.}, 2003 WL 21406289, at *3 (C.D. Cal. 2003).
  \item[111.] For example, the \textit{eBay} court found temporary dispossession of limited cyber-resources from unwanted searches on eBay’s web site sufficient to constitute trespass. \textit{See eBay, Inc. v. Bidder’s Edge, Inc.}, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).
  \item[112.] \textit{Ticketmaster}, 2003 WL 21406289, at *2 (describing the spider function of Tickets.com).
  \item[113.] \textit{See Compuserve, Inc. v. Cyber Promotions, Inc.}, 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (finding unwanted electronic mailings demand disk space and processing power of plaintiff’s computer equipment). By using the plaintiff’s computing resources for their unauthorized electronic mailings, the defendant denied use of these resources to the plaintiff’s customers, thereby diminishing the value of that equipment sufficient to sustain trespass to chattels claim. \textit{Id.}
\end{itemize}
another’s resources, even web site resources, is a use of another’s personal property not recognized under the law. 114

Other courts have addressed the unauthorized use of a web site’s resources by classifying it as a trespass. 115 For example, in Register.com, Inc. v. Verio, Inc., 116 the Southern District of New York found the defendant’s unwanted search robot occupied some of the targeted web site’s capacity; this was sufficient to establish the possessory interference needed to establish a trespass to chattels claim, and therefore, justify an injunction to stop the unauthorized activity. 117 The eBay court also recognized the problem of permitting even the use of limited web site resources by unwelcome visitors. 118

Neither party in eBay disputed that eBay’s server and its capacity were personal property and the Bidder’s Edge searches used a portion of this property. Even if, as Bidder’s Edge argued, its searches used only a small amount of eBay’s computer system capacity, the eBay court held that Bidder’s Edge has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. 119

Allowing unauthorized use of web site resources to continue unabated is the equivalent of declaring open season on cyber property, giving uncompensated rights to all-comers for the use of a web site’s limited resources. 120 Trespass to chattels is intended to give owners of personal property redress for another’s actions that interfere, even temporarily, with

114. See eBay, 100 F. Supp. 2d at 1071. eBay estimated the total load on their servers from the activities of Bidder’s Edge at between 1.11% and 1.53% of the total load on their servers. Id. at 1064. Even if a party’s actions use only a small portion of another’s web site resources, it creates an actionable trespass. Id. at 1071. “The law recognizes no such right to use another’s personal property.” Id.

115. See, e.g., Compuserve, 962 F. Supp. at 1015 (finding claim for trespass based on defendant’s transmission of unsolicited e-mail to plaintiff’s systems); eBay, 100 F. Supp. 2d at 1058 (finding trespass claim based on plaintiff’s partial use of defendant’s web site resources).


117. See id. at 250 (holding that, while plaintiff was unable to measure how much their system’s capacity was reduced, continued possessory interference with plaintiff’s web site resources was sufficient to merit injunction against defendant’s actions).

118. See eBay, 100 F. Supp. 2d at 1071 (noting use of even a small percentage of plaintiff’s processing capacity deprives it of right to use that capacity for their own purposes).

119. Id.

120. See Epstein, supra note 15, at 83 (noting in similar cases, “when the dust settles, if these defendants had been allowed to continue just as they are, then the upshot is that the defendant is entitled to receive an uncompensated compulsory license to use the equipment of the plaintiff for his own advantage.”).
their rightful ownership of that property — even if that property resides in cyberspace.¹²¹

D. Claims to Protect a Web Site Owner’s Possessory Interests in Their Site Should Not Be Preempted by Federal Copyright Claims

Critics of the cyber-trespass doctrine claim a web site owner’s assertion of property rights to protect their physical computer systems is, in effect, an effort to protect the data on those systems.¹²² In both eBay and Ticketmaster, for example, the information the defendants sought was purely factual, and not a generally copyrightable expression.¹²³ The successful use of trespass claims would allow these companies, and others like them, to prevent competitors from accessing their data, creating what critics term an “end-run” around copyright laws by placing state trespass claims before federal copyright law.¹²⁴

¹²¹. See PROSSER ET AL., supra note 38, at 85. Trespass to chattels is unique in that it allows redress to cover the unauthorized use of personal property that falls short of conversion:

Its chief importance now, is that there may be recovery . . . for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.

Id.

¹²². See Merrell, supra note 30, at 675 (noting eBay first brought its court action against Bidder’s Edge under copyright laws, which was dismissed). Ticketmaster also unsuccessfully claimed copyright violations from Tickets.com’s use of its information. See Ticketmaster Corp. v. Tickets.com, Inc., 2003 WL 21406289, at *5 (C.D. Cal. 2003) (noting information Ticketmaster sought to protect was unprotected, and publicly available factual event information was not protected under Copyright Act).

¹²³. See eBay, 100 F. Supp. 2d at 1072 (noting dismissal of eBay’s earlier copyright infringement claim). See also Ticketmaster, 2003 WL 21406289, at *5 (discussing Ticketmaster’s copyright infringement claims). The copyright protection for factual compilations is very thin. See Feist Publ’ns, Inc., v. Rural Tel. Svc. Co., 499 U.S. 340, 349 (1991) (holding phone listings compiled in phonebook not copyrightable information). “[N]o matter how much original authorship the work displays, the facts and ideas it exposes are free for the taking.” Id. The copyright “assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work.” Id. at 349-50. This leaves businesses and web sites that compile information unable to claim copyright protection for this information. See Merrell, supra note 30, at 696.

¹²⁴. See Merrell, supra note 30, at 697 (“[t]his end-run around the laws of copyright is inconsistent with federal copyright laws as interpreted in Feist and, under the Supremacy Clause, should be preempted.”).
If a state law cause of action, such as trespass, involves work that falls within the federal Copyright Act, the state cause of action is preempted if the rights being asserted under that state law are "equivalent" to those protected under copyright law. To hold a state claim is not "equivalent" to a copyright claim, the state claim must have an additional element that changes the nature of the action so that it is qualitatively different from a copyright infringement claim. The rights protected under trespass claims are not equivalent to the rights protected under copyright law, thus providing the extra element needed to make these claims qualitatively different from a copyright infringement claim. These claims are not about the use of information, but rather about how that information is obtained.

Critics rely on cases such as Sony Computer Entertainment, Inc. v. Connectix Corporation and Sega Enterprises Ltd. v. Accolade, Inc. to support the argument that the right to make fair use of factual information allows certain non-permissible activities, like copying copyrighted data to extract the public domain information, as support for permitting unauthorized access to a web site in order to gather public domain information. Access to factual information, however, even in the public domain, is not protected by copyright. The "fair use" doctrine does not apply in these circumstances. See, e.g., id. at 1073. The eBay court limited its injunction to the means used by Bidder's Edge to obtain the data from eBay. See id. ("[n]othing in this order precludes BE from utilizing information obtained from eBay's site other than by automated query program, robot, web crawler or similar device."). Other similar web-based copyright claims have similarly been dismissed. See, e.g., Associated Press, Not All Web Protected, MIAMI HERALD, Apr. 10, 2004, at B8 (describing ruling by Florida federal district court), available at 2004 WL 75366787. A U.S. district court in Florida held that a web site that aggregates yacht listings, photos, and product descriptions from other web sites did not violate the copyrights held by the originating web sites. See id. The web site, YachtWorld.com, used a software program to harvest information from other web sites to compile its listings of yachts for sale. See id. These listings were comprised of photos, descriptions, and price listings of yachts available for sale on a number of other web sites, including the plaintiff's Boats.com web site. See id. The YachtWorld.com court ruled that this data was unprotected by copyright law and YachtWorld.com's use did not infringe on any Boats.com copyrights. Id. (noting that copyright to yacht photos and descriptions were held by individual yacht owners, not plaintiff).

125. See Kodadek v. MTV Networks, Inc., 152 F.3d 1209, 1212 (9th Cir. 1998) (holding state claim for unfair competition preempted by federal copyright law).


127. See eBay, 100 F. Supp. 2d at 1072 (holding right to exclude others from using physical personal property under trespass law not equivalent to rights protected by copyright).

128. See, e.g., id. at 1073. The eBay court limited its injunction to the means used by Bidder's Edge to obtain the data from eBay. See id. ("[n]othing in this order precludes BE from utilizing information obtained from eBay's site other than by automated query program, robot, web crawler or similar device."). Other similar web-based copyright claims have similarly been dismissed. See, e.g., Associated Press, Not All Web Protected, MIAMI HERALD, Apr. 10, 2004, at B8 (describing ruling by Florida federal district court), available at 2004 WL 75366787. A U.S. district court in Florida held that a web site that aggregates yacht listings, photos, and product descriptions from other web sites did not violate the copyrights held by the originating web sites. See id. The web site, YachtWorld.com, used a software program to harvest information from other web sites to compile its listings of yachts for sale. See id. These listings were comprised of photos, descriptions, and price listings of yachts available for sale on a number of other web sites, including the plaintiff's Boats.com web site. See id. The YachtWorld.com court ruled that this data was unprotected by copyright law and YachtWorld.com's use did not infringe on any Boats.com copyrights. Id. (noting that copyright to yacht photos and descriptions were held by individual yacht owners, not plaintiff).

129. 203 F.3d 596 (9th Cir. 2000).

130. 977 F.2d 1510 (9th Cir. 1993).

131. Both Sony and Sega held reverse-engineering of the plaintiff's copyrighted code was permissible "fair use" of that code since it was the only way in which the unprotected elements within the code could be obtained. See also Ticketmaster Corp. v. Tickets.com, 2003 WL...
domain, can be legally curtailed. In *ProCD, Inc. v. Zeidenberg*, the Seventh Circuit held the terms of a “shrink wrap” software license, which prohibited the commercial use of a phone listing database, were sufficient to limit the use of public domain information contained in the database. Use of information, even factual data, on a web site is similarly governed by that site’s terms of use, and therefore subject to limitations imposed by those terms.

Some cases may also be able to rely on a defined exception to federal copyright protection because some public information may be protected as “hot news,” allowing unauthorized use of that information by a competitor to give rise to a misappropriation claim. First recognized by the U.S. Supreme Court in *International News Service v. Associated Press*, this exception applies to cases where:

(i) a plaintiff generates or gathers information at a cost; (ii) the information is time-sensitive; (iii) a defendant’s use of the information constitutes free riding on the plaintiff’s efforts; (iv) the defendant is in direct competition with a product or service offered by the plaintiffs; and (v) the ability of other parties to free-ride on the efforts of other plaintiff or others would so reduce the incentive

---


132. 86 F.3d 1447 (7th Cir. 1996).

133. See id. The *ProCD* court found the shrink wrap license terms on the plaintiff’s CD-ROM constituted a sufficient contract between ProCD and a user of the CD-ROM (the defendant). Id. at 1452-53. The *ProCD* court noted that enforcement of the limitations of these license terms does not withdraw any information from the public domain. Id. at 1455. “Everyone remains free to copy and disseminate all 3,000 telephone books that have been incorporated into ProCD’s database.” Id. Licenses help facilitate distribution of the databases, making the information even more readily available, and “serve the same procompetitive functions as does the law of trade secrets.” *ProCD*, 86 F.3d at 1455 (quoting Rockwell Graphic Systems, Inc. v. DEV Industries, Inc., 925 F.2d 174,180 (7th Cir. 1991)).

134. See Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 246 (S.D.N.Y. 2000) (holding that submitting query to Internet database indicates agreement to abide by stated terms of use for information retrieved from that database).

135. See Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974 (E.D. Cal. 2000) (holding charges competitor violated the unfair competition statute by downloading concert information off plaintiff’s web site not preempted by the Copyright Act since information was protected as “hot news”).

to produce the product or service that its existence or quality would be substantially threatened.\textsuperscript{137}

While it may not apply to all cyber-trespasses, the immediate nature of data on the Internet can make this exception particularly relevant in many of these cases.\textsuperscript{138} In \textit{Pollstar v. Gigmania, Ltd.},\textsuperscript{139} a federal court in the Eastern District of California applied the "hot news" exception to a cyber-trespass case.\textsuperscript{140} In \textit{Pollstar}, the plaintiff claimed the compilation of concert information on their web site was up-to-the-day time-sensitive information, which they assembled and posted at great time and expense.\textsuperscript{141} The defendant, Gigmania, downloaded concert information from the Pollstar site, and posted the information on its competing site.\textsuperscript{142} The \textit{Pollstar} court found there was a sufficient showing by the plaintiff to put the question of whether this was or was not "hot news" before a jury.\textsuperscript{143} Despite the similarities between the cases, the Central District of
California did not address a hot news argument in its *Ticketmaster* ruling.\(^{144}\)

**IV. CONCLUSION**

The freewheeling environment of cyberspace is often likened to the lawlessness of the "wild West."\(^{145}\) Even in the wilds of the old West, however, citizens recognized the societal need to protect personal property and did so with brutal, often fatal, consequences for those unfortunate enough to be caught infringing on another's property rights.\(^{146}\) The rather idealistic nature of the "wild West" metaphor for Internet freedoms conveniently overlooks the value of the rule of law — even on the cyber-

---

144. *See Ticketmaster, Corp. v. Tickets.com, Inc., 2003 WL 21406289 (C.D. Cal. 2003).* Ticketmaster brought copyright claims on three grounds. *Id.* at *4. First, Ticketmaster claimed that the momentary copying of the electronic signals used to generate the visual representation to the viewer of Ticketmaster's interior web pages was copyright infringement. *Id.* Second, Ticketmaster claimed that the URLs copied and used by the defendant to provide deep links to its site were copyrightable material. *Id.* Third, Ticketmaster claimed that the deep linking caused unauthorized display of their event pages. *Id.* The *Ticketmaster* court granted a summary judgment for the defendant on all of Ticketmaster's copyright claims. *Ticketmaster, 2003 WL 21406289,* at *6.


Of the many metaphors that have been applied to the Internet, the most prominent and influential has been the imagination of the Internet as a separate, new physical place known as "cyberspace" and its comparison to America's Western Frontier. This "Western Frontier" metaphor is both powerful and persistent... The West's remoteness ensured the absence of legal and social constraints associated with the civilized East... One can see the Internet in a similar way. Cyberspace "pioneers" experience the Internet as a special place devoid of the rules and constraints of "real space." This makes cyberspace a place where people find freedom from real space rules.


146. "Claim jumping" and horse theft were the most common frontier crimes — both of which were most often punishable by death. *See M.J. Welch, History of Douglas County Nevada, NEGen Web Project — Douglas County, available at http://www.rootsweb.com/~nedougla/html/douglas1.htm* (last visited Mar. 3, 2004). When early western settlements were made, lands were not yet formally surveyed, and settlers formed "claim clubs" to define and protect their property. *Id.* The methods of these clubs in settling claim disputes was described as "extremely effective, if unorthodox," applying swift and often violent vigilante justice. *Id.* Horse thievery was also often handled with similar vigilante justice — ending with horse thieves hanging from the nearest available tree limb. *Id.*
The historical rules of trespass, when permitted to evolve and meet the changing demands of an evolving society, provide a somewhat more predictable and civilized set of rules, and can provide the same benefits in cyberspace that they provide in the physical world.

Activity in cyberspace is currently governed by a complex mixture of common law, statutory regulations, voluntary standards, and customs. While informal and often voluntary rules proved sufficient to govern the Internet when it was a collegial online research community, this hodgepodge of regulation may not always produce satisfactory results in what is becoming an increasingly commercial and competitive environment. Trespass doctrine helps to fill the gap by addressing the problem of parties using the property of another for their own purposes, thereby preventing the taking of property rights that the law does not allow. With well-established legal principles to govern the limitations of their actions, parties in many of these disputes will work out their problems in a reasonable fashion, and for their mutual benefit. For example, less than a month after the issuance of the injunction in eBay, the company entered into a mutual agreement with another auction aggregator, BidXS.com, to permit it to search eBay’s site and include eBay auction listings on the BidXS.com web site. Certainly, there are a great degree

147. See Yen, supra note 145, at 1212-13 (noting the shortcomings of the Wild West metaphor). “This troubling use of the Western Frontier metaphor conveniently overlooks historical episodes of injustice and exploitation in the West that appropriate legal regulation might have prevented.” Id. at 1213.

148. Richard Epstein referred to this process as legal incrementalism where new forms of technology create new forms of resource uses, and property law emerges to govern the transactions between persons in taking advantage of these new technological possibilities. See Epstein, supra note 15, at 73-74. Epstein noted that, when properly applied, the rules of trespass “carry over to cyberspace without missing a beat.” Id. at 81.

149. See Caffarelli, supra note 4, ¶ 1 (noting confusion and uncertainty of Internet users when sorting out their rights in cyberspace).

150. Id. (“[a]s the Internet becomes even more commercial, the need for formalistic, predictable legal standards will increase”). “While some people may view the Web as a utopian environment, where ideas and information are readily and freely exchanged, others may see it as a horrific nightmare, where goods and wares are stolen by thieves who cannot even be seen.” Blanke, supra note 4, at 647.


152. Since the issuance of the injunction in eBay, the company has reached licensing agreements with similar auction aggregation sites, like PriceRadar and BidXS.com, allowing searches of their sites and listing of their auctions along with the auctions on other competing sites. See BidXS Signs Agreement with eBay (June 30, 2000), at http://www.prweb.com/releases/2000/6/prweb15948.php; see also Ken Cimino, Price Radar Gains Access to eBay Listings,
of technical complexities that can be injected into these cyber-trespass cases, but in the end, the laws which protect an individual’s rights in the real world often work with equal satisfaction in cyberspace.  

INTERNET.COM (Apr. 26, 2000), at http://siliconvalley.internet.com/news/article.php/348381. Other similar cases have also settled amicably following court-issued injunctions. See, e.g., Ahles, supra note 54, at C3. Three months following an injunction by a federal court to stop FareChase from accessing American Airline’s web site to collect fare information, the companies reached an agreement to allow FareChase access to American Airline’s AA.com web site and ability to book American Airlines fares through FareChase’s web software. Id. (describing settlement benefits for both parties).


So long as we keep our eye on the ball, we do not have to be fearful of the imagined consequences that will follow by taking the older rules of trespass and carrying them over to the brave new world of cyberspace, which, when all is said and done, for legal purposes at least, is neither as brave nor as new as it first appears.

Id.