Washington Law Review

Volume 79
Number 1 *Symposium: Technology, Values, and the Justice System*

2-1-2004

Crafting a License to Know from a Privilege to Access

Jane K. Winn
University of Washington School of Law

CRAFTING A LICENSE TO KNOW FROM A PRIVILEGE TO ACCESS

Jane K. Winn*

Should the doctrine of trespass to chattels[1] apply to unauthorized access to Internet facilities? If it does, then the property rights of the owners of computers connected to the Internet may be vindicated, but at a cost of diminished public access to information posted on the Internet. If it does not, then incentives to invest in the kind of commercial facilities that now largely constitute the Internet may be undermined, but the public interest in knowledge gleaned from information posted on the Internet will be protected. Although trespass to chattels has been derided as an anachronism ill-suited to the Internet,[2] and its application to Internet activities rejected in some recent cases,[3] other cases have held decisively that its application gives appropriate recognition to the rights of owners of computer equipment connected to the Internet.[4] In order to

---

* Director and Professor, Shidler Center for Law, Commerce & Technology, University of Washington School of Law. Thanks to William Edmundson, Brad Handler, and Jay Monahan for helpful comments.

1. Trespass to chattels is defined as the unauthorized, intentional, and substantial use of or intermeddling with another's tangible personal property. RESTATEMENT (SECOND) OF TORTS §§ 217–218 (1965).

2. "Trespass to chattels is somewhat arcane and suffers from desuetude." Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 247 (Cal. Ct. App. 2001), *rev'd*, 71 P.3d 296 (Cal. 2003). Many academic commentators have criticized the application of trespass to chattels doctrine to the Internet. *See, e.g.*, Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27 (2000); Edward W. Chang, *Bidding on Trespass:* eBay, Inc. v. Bidder's Edge, Inc. *and the Abuse of Trespass Theory in Cyberspace Law*, 29 AIPLA Q.J. 445 (2001); Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right To Exclude Indexing*, 26 U. DAYTON L. REV. 179 (2001); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433 (2003); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561 (2001); Maureen A. O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information?*, 53 VAND. L. REV. 1965 (2000) [hereinafter O'Rourke, *Shaping Competition*]; Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421 (2002).

3. *See, e.g.*, Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH (VBKx), 2003 U.S. Dist. LEXIS 6483, at *12 (C.D. Cal. 2003); Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003).

4. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1072 (N.D. Cal. 2000); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017 (S.D. Ohio 1997). Some academic commentators have applauded this trend. *See, e.g.*, Richard Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73 (2003);

safeguard the "license to know" factual information posted to the Internet that the public currently enjoys, courts should recognize an individual privilege to access Internet resources in a reasonable manner.

Given that trespass to chattels is unlikely to disappear from the Internet landscape any time soon, refinements are needed to keep the doctrine's scope within reasonable bounds and to make its application more predictable. The California Supreme Court recently imposed such a limitation on its application by holding that liability for trespass should be found only if the Internet access at issue significantly impairs the functions of another's computer equipment or, if widely replicated, would so impair it.[5] However, this attempt to restrict the scope of earlier rulings may prove to be at least as contentious as the holdings of the cases it purports to limit, and so is unlikely to staunch the flow of controversy.

The California Supreme Court focused on the functional impact that unauthorized access has on computer equipment owned by the party objecting to the access. A more helpful refinement of trespass doctrine might be found by considering instead which forms of access equipment owners have consented to merely as a consequence of connecting their equipment to the Internet. In every case in which trespass to chattels has been raised as an issue, before filing suit the equipment owner had demanded in no uncertain terms that the unauthorized access stop immediately, so the accessing party obviously cannot rely on a defense of express or implied consent. Courts could instead recognize a form of "constructive" consent to certain reasonable forms of access[6] that would defeat a claim of trespass. While such a finding of "consent" would not correspond to the actual subjective state of mind of the plaintiff bringing a trespass to chattels claim, it would have the benefit of refocusing attention on the social significance of the public character of the Internet, and hold the owner of computer equipment connected to the Internet accountable for having made the choice to create that connection.

Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217 (1996); Richard Warner, *Border Disputes: Trespass to Chattels on the Internet*, 47 VILL. L. REV. 117 (2002); I. Trotter Hardy, *The Ancient Doctrine of Trespass to Web Sites*, 1996 J. ONLINE L. art. 7 (1996), *at* www.wm.edu/law/publications/jol/95_96/hardy.html.

5. *Hamidi*, 71 P.3d at 296, 306.

6. The California Supreme Court came close to doing this. *Id.* at 308 ("Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes.").

One of the most significant problems created by the application of trespass to chattels doctrine to unauthorized Internet access disputes is its overbreadth. Trespass doctrine lacks the nuances normally found in intellectual property law to balance competing public and private interests in the exploitation of ideas and knowledge. Overbroad grants of rights in information have a chilling effect on the progress of science and the dissemination of knowledge generally.[7] Trespass doctrine vindicates the property rights of equipment owners at the expense of the "ease and openness of communication"[8] that has always been the hallmark of the Internet. Overzealous application of trespass doctrine obscures the fact that some forms of Internet access must be privileged if the unique public character of the Internet is to be preserved. Such a privilege should be limited in scope in recognition of the role played by private parties in maintaining the Internet today. The recognition of this privilege, however, should not be made contingent on the voluntary acquiescence of private parties.

Recognizing a defense to a claim of trespass in Internet cases based on a finding of constructive consent provides a doctrinal basis for privileging some forms of access while acknowledging a right to exclude certain other forms of access. Focusing attention on the public character of the Internet and assigning a clear legal significance to the equipment owner's deliberate choice to participate in that arena provide a more secure legal foundation for such a privilege to access than the "functional impairment" standard offered by the California Supreme Court. The contours of such a doctrine of constructive consent to Internet access are suggested by the terms of the license eBay offered to Bidder's Edge as discussed below—access by individual Internet users or its functional equivalent. This Article suggests that a defense based on constructive consent can complement the limitation imposed by the California Supreme Court to further limit the scope of trespass doctrine in Internet arenas, increase the predictability of the doctrine's application in new disputes, and help to protect important public interests in free and open access to Internet resources.

---

7. *See, e.g.*, J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997) (arguing that an intellectual property right in data will be harmful to science and education if based on the labor expended in building the database instead of innovation contained in the data).

8. *Hamidi*, 71 P.3d at 311.

I. SETTING THE STAGE: *EBAY, INC. V. BIDDER'S EDGE, INC.*

The first case to apply the doctrine of trespass to chattels to modern networked communication services involved the unauthorized use of access codes to make long distance calls.[9] That case held that teenagers who hacked into a long-distance telephone service's computer system and made unauthorized long distance calls using access codes thus obtained could be held liable for trespass to chattels.[10] The chattels at issue were the telephone access codes; the court declined to limit the application of trespass to chattels doctrine to intangible interests that were clearly associated with an interest in tangible property.[11]

The second case applying trespass to chattels to a modern networked communication system involved Cyber Promotions using the facilities of CompuServe, an Internet service provider (ISP), to send unsolicited commercial email (also known as spam) to the ISP's subscribers.[12] CompuServe's subscribers threatened to terminate their subscriptions unless it could stop Cyber Promotions from spamming them, and CompuServe undertook every technological measure at its disposal in a fruitless attempt to block Cyber Promotions' communications.[13] The court found that Cyber Promotions' spamming constituted trespass to chattels, the chattels in question being CompuServe's computer equipment, because the activity deprived CompuServe of the economic value of the equipment even though it did not lose possession of it.[14] The court rejected the argument that Cyber Promotions' access was privileged because CompuServe had consented to receive spam addressed to its subscribers, finding instead that whatever consent might be inferred from connecting its equipment to the Internet had been revoked by communications from CompuServe to Cyber Promotions.[15]

Perhaps the most well-known case to apply the theory of trespass to chattels involved a conflict between eBay and Bidder's Edge. eBay's primary business involves providing an Internet auction service that permits individuals to offer items for sale and also to purchase items

9. Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Cal. Ct. App. 1996).

10. *Id.* at 473.

11. *Id.* at 473 n.6.

12. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1018 (S.D. Ohio 1997).

13. *Id.* at 1019.

14. *Id.* at 1022.

15. *Id.* at 1024.

posted for sale.[16] eBay's business model focuses on creating a "community" of buyers and sellers; eBay does not itself offer for sale or guarantee any of the products offered on its site. Amazon.com and Yahoo! have similar auction sites, but eBay dominates the U.S. market for Internet auction services.[17] These Internet auction sites are designed to give unrestricted access to individuals wishing to browse the items offered for sale. To place an item for sale, or to bid on an item, it is necessary to register with the auction site, and the registration process requires individuals to manifest their assent to the auction site's terms and conditions of use.

A. Auction Aggregators: Licensed and Unlicensed

During the exuberant days of the dot com bubble, public interest in Internet auction sites such as eBay was exploding. A handful of dot com entrepreneurs devised the "auction aggregator" business model to permit individuals to search more than one Internet auction site simultaneously and to learn at once which site offered the best deal. There are no auction aggregators in operation today, but aggregators that once captured quite a bit of attention included www.auctionwatch.com, www.auctionferret.com, and www.auctionrover.com.

Given that eBay was the dominant player in the U.S. Internet auction site then as well as now, it could be expected to have ambivalent feelings about aggregator sites. Aggregators might increase the liquidity of auction markets created by its competitors; however, to the extent that eBay offered the largest selection and best prices, comparisons might have only increased its advantage over its competitors. To the extent that eBay's sellers would gain access to a larger group of prospective buyers through referrals from aggregators, however, they could be expected to support the work of the aggregator sites.

Perhaps in order to accommodate the wishes of its sellers, eBay made a practice of licensing to aggregators access to information about auctions taking place on eBay's site. These licenses were granted subject to certain restrictions designed to minimize the demands placed on eBay's own system by the aggregators, and to guarantee the accuracy

16. In 2000, eBay acquired Half.com, which provides a marketplace for buyers and sellers with fixed prices. In 2002, it acquired PayPal, the leading payment provider for Internet auction and consumer-to-consumer transactions.

17. Troy Wolverton, *At the Top of the Heap, eBay Still Must Look Down*, THESTREET.COM, July 24, 2003, *at* http://www.thestreet.com/pf/stocks/troywolverton/10101844.html.

of information being provided to aggregators' customers.[18] Aggregators were authorized to provide comparisons to aggregator site end users, provided that the demands they placed on eBay's site were equivalent to the demands that would have been placed on its systems if aggregators' customers had visited eBay's site directly. In other words, eBay would only authorize aggregators to perform "real time proxy searches," in which a query would be submitted for one item at a time, and the current price for that item would be provided to the aggregator's end user immediately. This type of proxy search both limited the demands that aggregator sites placed on eBay's servers and guaranteed that the aggregator's end user was provided with updated, accurate price information.

Many aggregators were willing to live within these constraints,[19] but some, including Bidder's Edge, were not.[20] Bidder's Edge's business model involved sending software robots (bots) onto eBay's site once every twenty-four hours to copy information about everything offered on the site. This information was sent back to Bidder's Edge and displayed in response to Bidder's Edge's end users' queries until another copy of all the listing information on eBay was made the following day. eBay objected both to the demands that the bots were placing on its system when copying all the listing information at once, and to the fact that Bidder's Edge's end users were often being shown inaccurate price information. When Bidder's Edge's end users clicked through an eBay listing only to find that the price had gone up since the Bidder's Edge copy of the data had been made, some of them blamed eBay for the unexpected change in price. eBay was also concerned that Bidder's Edge's wholesale approach to collecting data off its site might cause eBay to fail to perform some of its undertakings under its privacy policy, and might make it possible for Bidder's Edge to reuse information about "members" of the eBay community in ways that were expressly prohibited under the eBay User Agreement.

---

18. E-mail from Jay Monahan, Vice President, eBay, Inc., to author (Sept. 23, 2003) (on file with author).

19. Steven Bonisteel, *Auction Aggregator Gets OK To Search eBay*, NEWSBYTES, Dec. 1, 1999, *at* http://www.exn.ca/Stories/1999/11/25/02.asp.

20. *Auction Conflict Escalates*, WIRED NEWS, Oct. 11, 1999, *at* http://www.wired.com/news/business/0,1367,31850,00.html; Steven Bonisteel, *eBay's Battle with Auction Aggregators Heats Up Again*, NEWSBYTES, Nov. 4, 1999, *at* http://www.exn.ca/Stories/1999/11/04/01.asp.

eBay signaled its unwillingness to permit bots to trawl its site by using "robot exclusion headers." Many Internet businesses that rely on information collected by bots to function, such as search engines, program their bots to abide by restrictions placed by web site operators in robot exclusion headers. Bidder's Edge, by contrast, decided that it could ignore the content of eBay's robot exclusion headers with impunity because the information it was collecting from eBay's site was simply factual, and thus unlikely to be protected by copyright. In addition, because eBay's business model dictated that as much information as possible should be made publicly accessible on its site, and only participation in actual purchases and sales should require registration and the formation of a contract with eBay, Bidder's Edge could argue that the eBay User Agreement also did not apply.

eBay and Bidder's Edge entered into license negotiations that would have granted Bidder's Edge permission to perform real time proxy searches on behalf of its end users, but the negotiations were broken off without agreement. eBay then began to use all technological means available to it at the time to block Bidder's Edge's bots from accessing its site, but without success. eBay next filed suit against Bidder's Edge, seeking an injunction to prevent Bidder's Edge from sending unauthorized bots onto eBay's servers. The suit was based on various theories including trespass to chattels, false advertising, federal and state trademark dilution, computer fraud and abuse, unfair competition, misappropriation, interference with prospective economic advantage, and unjust enrichment. eBay was granted the injunction based on the trespass to chattels argument, but the court did not reach the other claims.[21] Bidder's Edge appealed to the U.S. Court of Appeals for the Ninth Circuit, but shut down its web site before the court heard oral arguments.[22] Shortly thereafter, Bidder's Edge paid eBay an undisclosed sum to settle the litigation.[23]

While the outcome in the *eBay, Inc. v. Bidder's Edge, Inc.*[24] case may have resolved the conflict between those two parties, the district court's ruling established an overbroad precedent. The district court's opinion does not place any limits on eBay's power to restrict access to its site

21. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1065 (N.D. Cal. 2000).

22. Jahna Berry, *Robots in the Hen House*, THE RECORDER, July 24, 2001, *at* http://www.law.com/regionals/ca/stories/edt0723_ip_robots.shtml.

23. *Id.*

24. 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

that eBay offered to Bidder's Edge in the failed license negotiations. eBay was willing to grant Bidder's Edge access to the information its customers wanted in a way that guaranteed that Bidder's Edge's customers were provided with only accurate price comparisons, but Bidder's Edge rejected the offer because it thought it could do better without a license.

B. Trespass to Chattels: Costs and Benefits

Applying the doctrine of trespass to chattels to the problem of unauthorized access to Internet resources has several benefits. It recognizes that most of the facilities that make up the Internet are now owned and operated by private parties. These are not eleemosynary institutions, and it is not their intention to donate their computers to the public once they connect them to the Internet. The doctrine of trespass to chattels also can be invoked if someone merely "intermeddles" with a chattel, a concept that is sufficiently vague to be capable of expanding to cover access to Internet resources. It puts the owner of the computer equipment in the driver's seat with regard to determining what access to its equipment is acceptable and what is not.[25] In the absence of such a theory, owners of computer equipment would have to consider the consequences of connecting their equipment to the Internet much more carefully, and, in all likelihood, some businesses would make the decision to withdraw their systems from full participation in the Internet in order to maintain an acceptable level of control over their networks.

These benefits notwithstanding, trespass to chattels fails to provide an adequate mechanism to balance the competing claims of Internet resource providers and Internet resource users. Asking whether an unauthorized electronic access to data stored in digital form on a server is equivalent to an unauthorized use of a toothbrush does not provide a rational basis for the development of the law in this area.[26] The doctrine of trespass to chattels was considered archaic and underdeveloped before

---

25. *See* Epstein, *supra* note 4.

26. The Restatement (Second) of Torts comments:

> There may, however, be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition. Thus, the use of a toothbrush by someone else may lead a person of ordinary sensibilities to regard the article as utterly incapable of further use by him, and the wearing of an intimate article of clothing may reasonably destroy its value in his eyes. In such a case, the intermeddling is actionable even though the physical condition of the chattel is not impaired.

RESTATEMENT (SECOND) OF TORTS § 218 cmt. h (1965).

its sudden burst of fame in the Internet context, and its application to sophisticated computer technology is unlikely to produce profound insights into the character of social relationships mediated by technology and law. Unlike nuisance doctrine, it does not require the explicit balancing of the competing public and private interests affected by the regulation of Internet access, substituting a private, commercial decision-making process for a more public, participatory process characteristic of the Internet in its early days.[27]

Perhaps the most appropriate theory for granting eBay the relief it sought against Bidder's Edge, and in similar cases, might have been some kind of a reverse passing off[28] "cold news" variation of the "hot news" misappropriation doctrine established in *International News Service v. Associated Press*.[29] In *International News*, the U.S. Supreme Court held that a rival news service could not copy news stories and resell the information even though the news stories lacked copyright protection.[30] The precise contours of misappropriation are somewhat unclear, but it seems at a minimum to grant a "quasi-property right" to the party claiming misappropriation, and to recognize the value of time and effort spent creating something of economic value that is not recognized by existing intellectual property law doctrines.

Although the holding in that case has been limited to its facts by subsequent cases,[31] those facts share a common characteristic with the facts of the *eBay, Inc. v. Bidder's Edge, Inc.* dispute because a large part of the economic value of the commercial information in both cases was determined by its "freshness." In the *eBay* case, however, Bidder's Edge's behavior might have driven eBay's customers away, not because they could get product of equal value from Bidder's Edge, but because the Bidder's Edge business model involved serving up eBay prices over eBay's objection after they had become stale. Such a tenuous argument

---

27. *See* Burk, *supra* note 2.

28. Reverse passing off is the marketing of another's product under a claim that it is one's own; passing off is marketing of one's own product under another's mark, i.e., trademark infringement. *See, e.g.*, Dastar Corp. v. Twentieth Century Fox Film Corp., 539 U.S. 23, __ n.1, 123 S. Ct. 2041, 2045 n.1 (2003).

29. 248 U.S. 215 (1918).

30. *Id.* at 219.

31. *See, e.g.*, Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 843 (2d Cir. 1997); Cheney Bros. v. Doris Silk Corp., 35 F.2d 279, 280 (2d Cir. 1929); Nat'l Football League v. Delaware, 435 F. Supp. 1372, 1377 (D. Del. 1977); *cf.* 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 (1997).

would have been unlikely to support a claim for a preliminary injunction, however, leading eBay to emphasize its trespass claim as a more solid basis for a grant of an injunction.

If the case had been decided on a misappropriation theory instead of a trespass theory, the court might have articulated limits to eBay's discretion in deciding what type of access to grant visitors to its site. For example, the doctrine of misappropriation prohibits competitors from reusing information, but does not prohibit individuals in the general public from reusing the same information.[32] A holding based on a misappropriation or deceptive trade practices theory might have distinguished between prohibiting certain forms of access arising out of unfair competition and preserving open access for other Internet users not engaged in any form of unfair competition.

The controversy surrounding the appropriateness of applying trespass doctrine to Internet access disputes is unlikely to subside any time soon, nor is the inconsistency in the manner in which the doctrine has been applied likely to be eliminated soon. While it remains possible that Congress will act to resolve this turmoil by enacting legislation that balances the competing public and private interests fairly, it is unlikely that will happen in the near future. So both Internet site operators and visitors will likely be left struggling to make sense of the emerging jurisprudence of trespass to Internet facilities. Articulating more clearly the significance of the decision by the owner of computer equipment to connect it to the Internet may create a mechanism for establishing a better balance of public and private interests, thus diffusing some of the current controversy and providing greater predictability in the application of trespass doctrine.

II. A RIGHT TO EXCLUDE QUALIFIED BY A PRIVILEGE TO ACCESS

The debate over whether trespass to chattels should be applied to resolve disputes involving unauthorized Internet access grows more acrimonious with passing time. On the one side are the "propertization" advocates, arguing that property rights of owners of the computer equipment at issue should trump other interests, giving the property owners a unilateral right to veto any use of their equipment they do not like.[33] On the other side are the supporters of the idea of the Internet as

32. *Int'l News Serv.*, 248 U.S. at 236.

33. *See* Epstein, *supra* note 4.

an open, public space where the community interest in preserving that openness conditions the right of owners of computer equipment to connect to the Internet on their acceptance of pre-existing Internet social norms of openness.[34]

The degree to which the debate has become polarized is obvious from this comment by Justice Brown in her dissent in *Intel Corp. v. Hamidi*[35]: "Those who have contempt for grubby commerce and reverence for the rarified heights of intellectual discourse may applaud today's decision, but even the flow of ideas will be curtailed if the right to exclude is denied."[36] But the debate need not be so polarized. The attempt to frame each position in absolute terms distorts each argument and obscures a possible middle ground where the competing claims of equipment owner and Internet end user might be harmonized.

Recasting the arguments using Hohfeldian terminology of rights can help clarify this middle ground.[37] Hohfeld suggested his system for classifying different forms of legal relations to show when apparent conflicts among different legal interests were misleading.[38] In the case of unauthorized access to Internet sites, vindicating the property rights of equipment owners negates any possible right Internet site visitors might have to free and open access to information posted on the Internet. Vindicating the public interest in freely making use of information posted on the Internet negates any right of the equipment owner to exclude others from its equipment. While each side would like to claim a strong form of rights in support of its position, it may be more accurate to say that equipment owners have certain limited property rights bundled together with certain privileges and powers, while the end users clearly could also be found to have a privilege of access that the equipment owner must respect. Recasting the debate in these terms is merely a first step toward resolving the controversy, because even if equipment owners are prepared to concede that end users enjoy an

---

34. *See* Burk, *supra* note 2; Ruth L. Okediji, *Trading Posts in Cyberspace: Information Markets and the Construction of Proprietary Rights*, 44 B.C. L. REV. 545 (2003); O'Rourke, *Shaping Competition*, *supra* note 2.

35. 71 P.3d 296, 325 (Cal. 2003) (J. Brown, dissenting).

36. *Id.* at 325 (J. Brown, dissenting).

37. Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16 (1913); *see also* WILLIAM A. EDMUNDSON, AN INTRODUCTION TO RIGHTS, ch. V, at 149 (Cambridge University Press ed., forthcoming 2004); Alon Harel, *Theories of Rights*, *in* THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY (Martin P. Golding & William A. Edmundson eds., forthcoming 2004).

38. Hohfeld, *supra* note 37, at 18.

implied license to access public Internet sites, the scope of that license remains to be defined.

A. Right to Exclude

Property rights in tangible computer equipment should not be conflated with a much broader right to exclude Internet users from accessing information on public web sites. If web site operators have a right to exclude end users, then end users have a corresponding duty not to interfere with the web site operator's exercise of its right. This is because, using Hohfeld's taxonomy, "duty" is the jural correlative of "right."[39] But assigning strong rights and correlative strict duties in this manner is at odds with the reality of Internet use by both web site operators and end users. Web site operators connect their systems to the Internet precisely in order to avail themselves of the public character of the network for commercial advantage. If web site operators are concerned about controlling access to their equipment, then such control can be accomplished by technological means—albeit at a cost of reduced traffic to a site.[40] For example, eBay permits casual visitors to look at auctions without registering, but will only permit registered "members of its community" to actually participate in actions as buyers or sellers. In order to join the community, individuals are required to complete a series of web forms and click through a contracting interface, agreeing to be bound by eBay's User Agreement. Registered users have user IDs and passwords that they must use to participate in auctions. User IDs and passwords with little or no verification of the information provided is a very rudimentary form of access control. If eBay required more security, it could use other networking technologies such as "virtual private networks."[41]

When commercial parties choose to connect their computer equipment to the Internet without restricting access to that equipment through the use of technological access controls, they are choosing to participate in a public forum. The Internet's public character was

---

39. *See* EDMUNDSON, *supra* note 37, at 154; Hohfeld, *supra* note 37, at 30.

40. Orin S. Kerr, *Cybercrime's Scope Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) (statutes criminalizing unauthorized computer access should be interpreted as requiring the circumvention of a technological barrier to access rather than violating a contractual limitation on access).

41. *See, e.g.*, RITA C. SUMMERS, SECURE COMPUTING: THREATS AND SAFEGUARDS 353–58 (1997).

established long before commercial exploitation of the Internet was permitted. Prior to 1995, the National Science Foundation Acceptable Use Policy (AUP) applied to Internet activity, and prohibited commercial use unless the National Science Foundation (NSF) reviewed the use for consistency with its overall mission and granted permission for it.[42] At that time, the purpose of the Internet was "to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work."[43] As Kesan and Shah explain:

> The NSFNET (later known as the Internet) connected universities, federal agencies, public and private research laboratories, and community networks. While the NSFNET encouraged such diversity, it also had an Acceptable Use Policy (AUP). The AUP prohibited the use of the NSFNET for purposes not in support of research and education, a policy consistent with the NSF's mission. Nevertheless, a growing number of users wished to use NSFNET for purposes beyond research and education, a push for what the NSF termed "commercial use." The potential for commercial use of the Internet propelled regional networks to create for-profit spin-offs. These for-profit commercial networks would eventually form the basis for the privatized Internet backbone.[44]

So the first commercial uses of the Internet were possible because the NSF granted immunity from expulsion to for-profit entities that joined the Internet. Under that immunity, the number of for-profit service providers grew until 1995, when the NSF was able to withdraw its support for the Internet backbone and turn it over to private parties to operate.

Equipment owners that once accepted a mere immunity from expulsion in order to share in the benefits of Internet access are now trying to turn the tables on other Internet users and claim a right to exclude other Internet users at will. But this is too broad a claim of right:

---

42. National Science Foundation, *Acceptable Use Policy* (July 3, 1990), *available at* http://www.eff.org/Net_culture/Net_info/Technical/Policy/nsfnet_policy.old.

43. Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89, 112 (2001).

44. *Id.* at 111 (citing BRIAN KAHIN, *The NREN as Information Market: Dynamics of Public, Private, and Academic Publishing*, *in* BUILDING INFORMATION INFRASTRUCTURE 323–24 (Brian Kahin ed., 1993)).

a narrower claim of right that recognizes a privilege of access for ordinary end users is adequate to protect the equipment owner from unfair competition and hostile intrusions to their equipment that interfere with their commercial activities. A narrower claim of right more fairly balances the interests of equipment owners and ordinary end users by permitting web site operators only to restrict access by other commercial parties, not access by individual end users. Some form of implied license for individual end users must be recognized to prevent the destruction of the open, public character of the Internet in the name of commerce.

Granting web site operators a power to exclude other commercial actors from overbroad access to their sites, in lieu of a stronger right to exclude anyone from accessing their sites for any reason, assigns a realistic and appropriate significance to the equipment owner's free choice to connect its equipment to an open, public communications medium. In Hohfeldian terms, to say that someone has a power is not to say that anyone else has a duty; rather, someone else might incur a duty if the power is exercised.[45] Giving web site operators a power to fend off potential competitors permits them sufficient control over their equipment to protect its commercial value without depriving the general public of its ability to enjoy freely the open character of the Internet. If web site operators want to restrict access to their sites by the general public, then they can take concrete steps to restrict access to information on servers attached to the Internet, for example, by putting the information behind a firewall and implementing technological access controls. Many commercial web site operators, such as eBay, are unwilling to place these kinds of restrictions on casual visitors to its site, but do place these restrictions on anyone who would proceed from merely viewing information to transaction processing. The business decision regarding the design and implementation of access controls to Internet facilities should be assigned a legal significance in any subsequent dispute over whether a particular form of access was authorized.

B. Right to Access

Even the most vigorous opponents of the application of trespass to chattels to the issue of Internet access have not argued that Internet end

45. *See* EDMUNDSON, *supra* note 37, at 155.

users have a "right to access" Internet facilities.[46] Such a strong claim would imply that equipment owners have a duty to maintain the equipment so that end users' rights can be exercised.[47] Instead, opponents argue that end users should receive a broad grant of immunity from liability as a consequence of the equipment owner having made the decision to connect to the Internet. In the *eBay* case, this immunity would have prevented eBay from getting an injunction to stop Bidder's Edge's bots from copying and transmitting large quantities of information accessible on eBay's site before the court reached a judgment on the merits.

A commercial entity such as Bidder's Edge cannot claim that the type of access for which it demands immunity was an integral part of the public character of the Internet that eBay knowingly embraced. As early as 1994, a standard for robot exclusion was being developed informally to permit web site operators to communicate their desire to exclude software robots from their sites.[48] Bidder's Edge's decision to send bots to copy and transmit data from eBay's site for commercial exploitation on Bidder's Edge's site bears no resemblance to the types of access that would have been permitted under the NSF's AUP. By contrast, the terms of the license that eBay offered Bidder's Edge and that Bidder's Edge rejected bore a close resemblance to the types of access that would have been permitted under the NSF's AUP. Bidder's Edge rejected eBay's "reasonable access" license, however, and instead gambled on an aggressive claim that because it had the right to make unrestricted commercial use of the factual information on eBay's computers, eBay had no right to restrict its access to eBay's servers.

C. Privilege to Access from Constructive Consent

Consent may create a defense to a claim of tort liability by creating a privilege to engage in the conduct in question.[49] An end user has a plausible claim that any web site operator who has not articulated an

---

46. *See, e.g.*, Brief of Amici Curiae Electronic Frontier Foundation, Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (No. S103781), *available at* http://www.eff.org/Spam_cybersquatting_abuse/Spam/Intel_v_Hamidi/intel_v_hamidi_amicus.pdf; Burk, *supra* note 2; O'Rourke, *Shaping Competition*, *supra* note 2.

47. "[Hamidi] does not argue that he has a right to force unwanted messages on Intel." Intel Corp. v. Hamidi, 71 P.3d 296, 318 (Cal. 2003).

48. *See, e.g.*, Martijn Koster, *A Standard for Robot Exclusion* (Jun. 30, 1994), *available at* http://www.robotstxt.org/wc/norobots.html.

49. RESTATEMENT (SECOND) OF TORTS § 890 cmt. b (1965).

express policy governing access to its site has impliedly consented to any reasonable, conventional form of Internet access. However, this implied license alone cannot support the creation of a robust privilege of access for individual end users because a web site operator can revoke any implied consent at any time by notifying visitors that it has established a restrictive access policy.

The only way to create a robust privilege of access for the general public is to find constructive consent to access web sites based on a web site operator's choice to join the Internet without placing any functional restrictions on access to its site. Constructive consent is not a finding that consent exists as a factual matter, but rather is a legal fiction that asserts that something tantamount to consent does exist, and that it will be given the same legal effect as consent. While courts are often willing to find consent implied in light of parties' behavior in a given context, they are generally reluctant to invoke the notion of constructive consent without an extraordinary justification.[50] This general reluctance notwithstanding, a finding of constructive consent can be used to balance competing public policy objectives.[51] Here, the competing policy objectives are the need to allow web site operators to protect themselves against interference, and the public's need for open access to web sites. The notion of constructive consent shifts the obligation from the individual end user to ensure that his or her access is permitted to the web site operator to choose between granting the general public reasonable but unfettered access to its site and placing some form of functional access controls on its site.

In order to strike an appropriate balance between the interests of individual end users in preserving the public character of the Internet and the interests of commercial web site operators in preserving and exploiting the value of the equipment they have connected to the Internet, the notion of constructive consent must be limited to those situations where the public interest in unrestricted access is clear. The NSF's AUP provides a convenient starting point for the process of defining what "reasonable" individual access or its functional equivalent would be. But because AUP ceased to apply to Internet activities nearly a decade ago, it would be anachronistic to adhere too closely to its terms

50. *See, e.g.*, *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 19–20 (1st Cir. 2003); Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990).

51. *See, e.g.*, Murdza v. Zimmerman, 786 N.E.2d 440, 442–43 (2003).

in the search for a definition of access to Internet facilities so reasonable, it should always be privileged.

Requiring a finding that machine functions were neither actually impaired nor likely to be impaired as a result of wide replication of the offending form of access, as the California Supreme Court did in *Hamidi*, is an important element in recognizing a privilege to access public Internet facilities, but by itself is not a complete protection for that privilege. The focus of a court's analysis should be on the intent of commercial operators of computer equipment in making the decision to connect their facilities to the Internet, not on the impact that access has on machine functions. Focusing on intent and the social significance of the public character of the Internet creates a framework within which a privilege to access Internet resources can evolve with technological change while remaining consistent to its objectives.

III. RECENT TRESPASS CASES

The holdings of recent cases applying the doctrine of trespass to chattels to Internet access disputes veer from finding no privilege to access Internet sites to finding immunity from liability for clearly unauthorized access.[52] If Internet facility operators, by connecting their equipment to the Internet without technological access controls, are deemed to have consented to the technological equivalent of individual access, can this notion of constructive consent help to make sense of recent trespass cases that otherwise seem to veer back and forth between contradictory interpretations? As the following analysis makes clear, the privilege of reasonable access for individual Internet users or its functional equivalent unfortunately is not a silver bullet that magically resolves all the overbreadth problems inherent in applying trespass to Internet access disputes. It may nevertheless help to focus attention on which characteristics of the Internet commercial parties should be required to tolerate, however grudgingly, as a condition of maintaining an open connection between their equipment and the Internet.

---

52. Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH (VBKx), 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. 2003) (finding immunity from liability); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003); Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (Cal. Ct. App. 2001), *rev'd*, 71 P.3d 296 (Cal. 2003) (finding no privilege).

A. Register.com, Inc. v. Verio, Inc.

In *Register.com, Inc. v. Verio, Inc*,[53] a domain name registrar used trespass to chattels to stop unauthorized access to its site by a competitor. Although Register.com was required by its Registrar Accreditation Agreement (RAA) with the Internet Corporation for Assigned Names and Numbers (ICANN) to permit the use of domain name registration data for any lawful purpose, it was not permitted to allow the use of that data to enable the transmission of mass, unsolicited, commercial email (spam). Register.com worked with business partners to provide web hosting and other Internet services to its domain name registration customers. Verio, a provider of web hosting and other Internet services, used a software robot to collect information about recently registered domain names and then contacted the individuals who had registered them to offer them various Internet services. The manner in which Verio contacted Register.com customers was calculated to cause Register.com customers to believe Verio was, at a minimum, a business partner of Register.com when in fact it was a competitor. After Register.com learned, through complaints from its customers and business partners, that Verio was soliciting its customers in this manner, it demanded that Verio stop making such solicitations. When Verio would not agree to cease the solicitations, Register.com sought an injunction to stop Verio, pleading trespass to chattels, breach of contract, unfair competition, and unauthorized access under the Computer Fraud and Abuse Act. The court issued a preliminary injunction based on a finding that Register.com was likely to prevail on both the trespass to chattels and computer fraud claims.

The holding in *Register.com* has been controversial because the court did not require a showing that Verio's unauthorized access was actually interfering with the functioning of Register.com's equipment. Instead, the court accepted Register.com's argument that if Verio was allowed to continue this type of unauthorized access, the floodgates would open and there would be no end to the other companies using the same technique to harvest data from Register.com's system, at which point the functioning of its equipment would be impaired.

If the court had used the constructive consent approach, the terms of the RAA, which required Register.com to provide public access to its data except under two limited circumstances, might have provided

53. 126 F. Supp. 2d 238 (S.D.N.Y. 2000).

evidence of what access Register.com could be deemed to have consented. Instead, because Verio had no rights as a third-party beneficiary under the RAA, the court rejected evidence that Register.com's terms of use of its data were more restrictive than the RAA permitted.[54] However, subsequent to the *Register.com* lawsuit, ICANN revised the terms of the RAA, requiring domain name registrars not to give access to data for "transmission by e-mail, telephone, or facsimile of mass, unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers."[55] This revised RAA closely resembles the Register.com terms in effect at the time of Verio's unauthorized access, indicating that Register.com's terms of use were not unreasonable even if they did not conform to its obligations under the version of the RAA in effect at the time of the litigation. If the later standard of acceptable use of Register.com data was used as the standard by which constructive consent should be measured, then Verio's conduct would not have been privileged after all.

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

Ticketmaster Corp. v. Tickets.com, Inc.[56] considered the application of trespass doctrine to the problem of one commercial site linking to another without permission.[57] Ticketmaster is the largest company selling tickets to sporting and other entertainment events, and has both online and bricks-and-mortar operations; Tickets.com is one of its competitors, operating primarily online. Tickets.com provided visitors to its own web site information about events for which Ticketmaster was the exclusive sales agent by providing "deep links" into Ticketmaster's web site. These deep links permitted Tickets.com's visitors to avoid Ticketmaster's home page and directly access information about a particular event located deep within Ticketmaster's web site. In 2000, Ticketmaster unsuccessfully sought a preliminary injunction to stop Tickets.com from providing deep links into its site, claiming breach of

54. *Id.* at 248 (stating that the RAA expressly provided that no third party beneficiaries would be created by its terms).

55. Internet Corporation for Assigned Names and Numbers Registrar Accreditation Agreement (ICAAN RAA) § 3.3.5 (May 17, 2001), *available at* http://www.icann.org/registrars/ra-agreement-17may01.htm.

56. No. CV99-7654-HLH (VBKx), 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. 2003).

57. *Id.*

contract, copyright infringement, trespass to chattels, false advertising, and trademark infringement.[58]

In 2003, the same court granted summary judgment to Tickets.com on Ticketmaster's trespass to chattels and copyright claims, but denied summary judgment on the breach of contract claims.[59] Tickets.com sent a software robot onto the Ticketmaster web site to copy information about events, then discarded information such as logos, advertisements, and formatting, keeping only the factual information describing the events. The court rejected the idea that any unauthorized access by a software robot could give rise to liability for trespass when no impairment of the function of the equipment had been shown.

The notion of constructive consent would point toward the same result here because hypertext is one of the defining characteristics of the World Wide Web. The court found that Ticketmaster had not shown that it had suffered any damages, such as loss of advertising revenues, as a result of the deep links created by Tickets.com. While the holding in the case was based on the inability of Ticketmaster to make out any trespass claim at all based on failure to prove the element of damages, the lack of damages also supports a finding that the access by Tickets.com through deep linking was the functional equivalent of reasonable access by an individual user. Ticketmaster wanted anyone interested in events for which it was the exclusive agent to access its site from its home page, but when the original dispute arose in 1999, it had not implemented any access controls that would have required individual visitors to follow such a route.

C. Intel Corp. v. Hamidi

In *Intel Corp. v. Hamidi*, a disgruntled former employee used the Internet to criticize his erstwhile employer by sending emails to current Intel employees and by building a web site to disseminate his anti-Intel opinions on the World Wide Web.[60] After someone provided him with an electronic copy of Intel's employee directory, Hamidi sent emails on

58. Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. 2000).

59. *Ticketmaster Corp.*, 2003 U.S. Dist. LEXIS 6483, at *2 (finding immunity from liability). In 2000, the trial court found that Ticketmaster was unlikely to prevail on its breach of contract claim, but after additional discovery turned up new evidence that Tickets.com may have entered into a contract with Ticketmaster over the Internet the court in 2003 refused to enter summary judgment in favor of Tickets.com.

60. 71 P.3d 296 (Cal. 2003).

six occasions to anywhere from 8,000 to 35,000 employees, or a total of between 48,000 and 210,000 emails in all.[61] Hamidi's messages promised to remove recipients from the mailing list upon request, and he apparently complied with all such requests that he received.[62] Intel, however, was unwilling to wait for its employees to make such requests or simply to delete Hamidi's emails from their inboxes, and so demanded that Hamidi stop sending critical emails to its current employees.[63] At trial and on appeal,[64] Intel's request for an injunction was granted based on a trespass to chattels theory, notwithstanding the lack of a showing of any significant impairment of Intel's system's functioning. The California Supreme Court took a different view of trespass doctrine, and held that because there was no significant impairment of Intel's system's functioning, and because there was no indication that a flood of other former disgruntled employees were waiting to deluge it with emails, Hamidi was immune from liability under trespass doctrine.[65]

In determining whether Intel should be deemed to have consented to Hamidi's use of its equipment to send emails to its current employees, notwithstanding its vociferous objections, a crucial factor would seem to be the non-commercial character of Hamidi's communication. Although the California Supreme Court did not reach the issue of whether enforcement of a state law that interfered with Hamidi's exercise of his free speech rights would constitute impermissible state action under the First Amendment, unlike the *Register.com* and *Ticketmaster* cases, Hamidi was not a competitor of Intel, and his behavior did not raise unfair competition issues. On the other hand, if constructive consent creates a privilege for reasonable individual access of Internet facilities, it is unclear whether sending 48,000 to 210,000 emails constitutes reasonable individual use. A final factor suggesting that Intel should be deemed to have constructively consented to Hamidi's sending emails to its current employees is its failure to implement more effective and restrictive access controls. By granting its employees relatively free access to the Internet, Intel arguably entered into a public arena within

61. *Id.*

62. *Id.*

63. *Id.*

64. Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (Cal. Ct. App. 2001), *rev'd*, 71 P.3d 296 (Cal. 2003).

65. *Hamidi*, 71 P.3d at 311.

which it could be expected to tolerate the criticism of ex-employees such as Hamidi, at least in the absence of any showing that Hamidi's communications were impairing the function of its systems.

IV. CONCLUSION

The public character of the Internet can be protected by assigning a legal significance to decisions by commercial Internet users about how to make use of Internet technologies. Individual users of the Internet should have a license to access what is posted on the Internet that cannot be negated by arbitrary assertions of rights over information rooted in ownership of tangible computer equipment. Because the free flow of information has been a hallmark both of civil society and the Internet, that association between civil liberties and the institutional character of the Internet should be preserved notwithstanding the growing commercialization of Internet resources. Granting individual users a privilege to access information on the Internet in a reasonable manner would preserve the basic character of that association while still recognizing that the Internet is now sustained by private investment in computer equipment. Access by anyone other than individuals in a manner that approximated individual access would likewise be covered by an implied license created by constructive consent, but consent to access that differs in quality or quantity from that associated with individual users could be withdrawn. This license to access information would be in effect a privilege implied by law that limits the property rights of the owners of the equipment. Using the common law to articulate the scope of constructive consent to access by Internet users, and the privilege it creates, would help to clarify the social significance of the Internet itself and establish viable standards to safeguard its open, participatory character.