2002

Common Law and Statutory Restrictions on Access: Contract, Trespass, and the Computer Fraud and Abuse Act

Maureen A. O'Rourke
Boston University School of Law

COMMON LAW AND STATUTORY RESTRICTIONS ON ACCESS: CONTRACT, TRESPASS, AND THE COMPUTER FRAUD AND ABUSE ACT

Maureen A. O'Rourke[*]

I. INTRODUCTION

Is copyright law relevant to the terms of access to information? Certainly, few would seriously contend that breaking into a locked filing cabinet to obtain access to a manuscript is not sanctionable, even if the intruder had some purpose that copyright law would applaud with respect to the information contained in the manuscript itself. Many instinctively believe that one must pay the asking price and respect the terms that accompany a copyrighted work or face the consequences under some set of laws like copyrights or contracts. In short, society likely generally believes that market forces regulate the conditions of access to information with copyright law providing the background rules on use of that information.

At first glance at least, copyright law and practice support this view. Until enactment of the Digital Millennium Copyright Act ("DMCA") (which generally protects the use of access control devices),[1] copyright law had little to say about access, at least explicitly.[2] Copyright law provides a statutory structure that endows authors with a bundle of rights that they may or may not choose to license.[3] Authors generally transfer

---

* Professor of Law and Associate Dean for Administration, Boston University School of Law. Thanks to Phil McConnaughay and Bruce Smith for inviting me to participate in the 2002 Chicago International IP Conference. Thanks also to Professors Christine Galbraith and Michael Meurer and my research assistants Stacy Blasberg and Stephanie Smith for their help.

1. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.). Protection for access controls is set forth primarily in 17 U.S.C. § 1201 (2002).

2. This is, of course, overly simplistic. Many of the limitations on copyright's exclusive rights are targeted toward increasing access to copyrighted works. *See generally*, 17 U.S.C. §§ 107-121 (2002) (setting forth those limitations). The point is merely that copyright law does not, as a matter of course, specifically regulate the manner in which users obtain access to copyrighted works.

3. Section 106 of the Copyright Act defines this bundle, which includes the rights to exclude others from reproducing the work and making derivative works of it. *Id.* at § 106.

one or more of their rights to distributors, like publishing houses, in return for some compensation. These distributors set the price of access to the work. Consumers pay the price to obtain the work, and copyright law governs what uses they may make of it.

Sometimes though, distributors attempt by contract to further limit access and use by creating rights in addition to those that copyright law gives. Those who would be bound by such provisions occasionally argue that copyright law preempts their enforcement. Traditionally though, preemption cases have been highly technical, relatively few in number, and often decided in favor of the distributor/licensor.

However, reliance on the courts to decide questions of the relationship between the laws of copyright and contract has been increasing ever since vendors began to mass market pre-packaged software. This trend will continue as providers of information on the Internet use clickwrap or browsewrap agreements to regulate the terms of access to and use of information. Employing the courts to define the terms of the "bargain" will not cease until they have developed a consistent and predictable set of principles to evaluate such claims.

Furthermore, those who provide information on the Internet have begun to assert claims not grounded in contract law. Specifically, they have successfully used the common law tort of trespass to chattels and the federal Computer Fraud and Abuse Act ("CFAA")[4] to police access to and use of Web sites and the information contained therein.

In this brief article, I discuss these causes of action,[5] arguing that courts evaluating them have been less receptive than they should be to considerations of copyright policy. Courts should not adopt a perspective that cedes all questions of terms of access and use to laws other than copyright. Commentators, and indeed the courts themselves, have long accepted that copyright law seeks to encourage not only authorship but also the dissemination of creative output in the name of furthering progress. Copyright law thus has something to say about access and terms of use. I offer here some suggestions for methods of analysis that courts might employ to vindicate copyright policy while providing some level of predictability desired by those who create and market copyrighted works.

4. 18 U.S.C. § 1030 (2002).

5. Certainly the DMCA provides a potent tool that protects access control measures. Commentators have written extensively on that statute. Here, I concentrate on those causes of action that implicate "low-tech" access control measures. These inexpensive means of access control may ultimately prove more ubiquitous than those the DMCA protects, and therefore merit attention.

II. CONTRACT: CLICKWRAPS, BROWSEWRAPS — AND COPYRIGHT POLICY

Entire industries like the entertainment business are built around copyright licensing. That contracts would regulate access to and rights in information is neither new nor even particularly noteworthy. What is arguably new is the extent to which information providers use standard forms with terms imposing greater restrictions than copyright law. The ubiquity of such terms, if enforceable, would create an effect unlike that traditionally associated with contracts. Rather than simply binding two parties to an agreement, the terms effectively bind the world because no one may access the information without agreeing to the contract. By creating more extensive rights than copyright law, private contracts begin to look like private legislation that conflicts with the public law. As parties litigate these contracts, courts will have to confront the issue of copyright preemption of contractual terms more often than in the past.

A. What Contract Law Would Say

Contract law has come a long way from the days in which models of contracting were based on a face-to-face exchange.[6] As technology began to enable long-distance communication, contract law had to address the increasing probability that it could not identify the moment of contract formation, and that no negotiation would take place at all. Rather, the offeree could buy the product only on a "take-it or leave-it" basis.[7] The general legal response has been to enforce bargained-for terms, while granting unbargained-for ones a presumption of enforceability that may be overcome by a showing of unconscionability.[8] This approach reflects an appreciation of both the pros and cons of standard form contracts. Although standard terms often reflect an efficient allocation of contractual risks, sometimes an unscrupulous business can use them to exploit consumers who, as a group, are unlikely to read them.[9]

On the Internet, firms commonly offer users clickwrap or browsewrap agreements containing standard terms. A clickwrap agreement requires the user to click on a button indicating agreement to

---

6. *See* James J. White, *Autistic Contracts*, 45 WAYNE L. REV. 1693, 1697-98 (2000) ("The classical model, one that is still practiced and is often held as the contracting prototype, is an interactive face-to-face exchange between an offeror and an offeree . . . .").

7. *See id.* at 1698 (noting that mail and phone permit interactive communication analogous to face-to-face bargaining but that "take-it or leave-it" deals have also existed since early times); *see also* Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 431 (2002) (stating that "[l]ikely ninety-nine percent of paper contracts consist of standard forms").

8. Hillman & Rachlinski, *supra* note 7, at 487 (setting forth the textual proposition and identifying it as "Llewellyn's framework").

9. *Id.* at 432-33.

the terms prior to obtaining the information.[10] A browsewrap associates agreement with some other act like downloading information or submitting a query: the particular terms are available somewhere on the site but the user need not view them to engage in the activity indicating consent.[11]

Courts generally uphold the clickwrap approach as a permissible means of forming an agreement because the user has an opportunity to review the terms before becoming bound by them.[12] Browsewraps, perhaps predictably, have fared somewhat less well, with the courts split on their enforceability.[13] Arguably, the trend is to consider a browsewrap enforceable if the site places the terms where the user is

10. Drew Block, News, *Caveat Surfer: Recent Developments in the Law Surrounding Browse-Wrap Agreements, and the Future of Consumer Interaction with Websites*, 14 LOY. CONSUMER L. REV. 227, 229-30 (2002) (noting that the agreement may appear when a user tries to download or install software); Ryan J. Casamiquela, Note, *Contractual Assent and Enforceability in Cyberspace*, 17 BERKELEY TECH. L.J. 475, 476 (2002) (stating that the box indicating agreement may appear at the end of the list of terms).

11. Block, *supra* note 10, at 230 (describing a browse-wrap as an approach in which a hyperlink can lead to the terms but the user is bound by them after moving past the home page regardless of whether or not the user clicks on the link and views the terms).

12. *See, e.g.*, Moore v. Microsoft Corp., 741 N.Y.S.2d 91 (N.Y. App. Div. 2002); Hughes v. McMenamon, 204 F. Supp. 2d 178 (D. Mass. 2002) (holding an AOL clickwrap enforceable and also citing other cases holding clickwraps enforceable); I.LAN Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002) (upholding a clickwrap when the parties had also signed a detailed agreement). The foundational case is *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996). Although often referred to as involving a shrinkwrap agreement, the case in fact also seemed to involve a clickwrap as each time the user ran the software, an initial screen appeared setting forth the license terms. *Id.* at 1450. Since *ProCD*, the courts have also shown an increased willingness to enforce shrinkwrap agreements that are included in the box in which the product ships. *See, e.g.*, Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997), *cert. denied*, 522 U.S. 808 (1997) (enforcing an arbitration provision in a boilerplate contract accompanying a computer); *Brower v. Gateway 2000*, Inc., 676 N.Y.S.2d 569 (App. Div. 1998) (same result as *Hill v. Gateway*); Rinaldi v. Iomega Corp., 1999 WL 1442014 (Del. Super. Ct. 1999) (holding a warranty disclaimer included inside computer Zip drive packaging enforceable). Finally, note that some vendors ostensibly take a combined click- and browsewrap approach. *See, e.g.*, Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1169-70 (N.D. Cal. 2002) (describing a contract to which users could agree by either clicking "I Agree" to the terms or by submitting certain information).

13. *Compare* Specht v. Netscape Comms. Corp., 306 F.3d 17 (2d Cir. 2002) (refusing, under California law, to enforce a contract formed by the act of downloading where the user did not have notice of the terms) *and* Ticketmaster Corp. v. Tickets.com, Inc., 54 U.S.P.Q. 2d 1344, 1346 (C.D. Cal. 2000) (addressing a breach of contract claim based on a browsewrap, providing that proceeding past the home page constituted assent, distinguishing the browsewrap from the shrinkwrap, and noting that: shrinkwraps are open and obvious and in fact hard to miss. Many web sites make you click on "agree" to the terms and conditions before going on, but Ticketmaster does not. Further, the terms and conditions are set forth so that the customer needs to scroll down the home page to find and read them . . . .It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site . . . .), *with* Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 982 (E.D. Cal. 2000) (refusing to dismiss a breach of contract claim based on a browsewrap license where the agreement was mentioned in small type on the home page and became effective when the user moved past the home page. The court stated that it was "hesit[ant] to declare the invalidity and unenforceability of the browse wrap license agreement" on a motion to dismiss) *and* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000) (upholding a browsewrap in which the user agreed to the terms by submitting a query when the terms were clearly posted and the defendant did "not argue that it was unaware of these terms, only that it was not asked to click on an icon indicating that it accepted the terms").

likely to see them, and the manner in which they become binding is reasonable.[14] Indeed, the drafters of the Uniform Computer Information Transactions Act ("UCITA") have taken just such an approach.[15]

The question of contract formation is however, at least partially analytically distinct from the enforcement of particular terms. How should courts address terms that restrict the use of information more than copyright law would? Should they enforce such terms or hold them preempted?

Contract law refuses to enforce terms that are unconscionable or that violate some other rule of law.[16] Generally, courts require elements of both procedural and substantive unconscionability before refusing to enforce a contractual term.[17] In a clickwrap or browsewrap agreement, the user most often has no other contact with the site. The only "procedure" involved in reaching agreement is the user's click or other act. If courts are willing to hold that this conduct forms a contract, the element of procedural unconscionability appears lacking.[18]

Procedural unconscionability refers to the absence of meaningful choice by one party.[19] Generally, courts will not use unconscionability as a device to level otherwise unequal bargaining power.[20] Instead, lack of meaningful choice "is usually founded upon a recipe consisting of one or more parts of assumed consumer ignorance and several parts of seller's

14. Casmiquela, *supra* note 10, at 487 ("Courts may . . . find consumer assent in the absence of a clicking acceptance if the consumer is somehow put on notice."); *see also Specht*, 306 F.3d at 35 (refusing to uphold a browsewrap while also noting, "Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms are essential if electronic bargaining is to have integrity and credibility"). The court's statement suggests that it might uphold a browsewrap if reference to the existence of the terms is conspicuous and it is clear to the user that a particular act indicates assent to those terms.

15. Uniform Computer Information Transactions Act § 211 (2001) (setting forth rules on when a licensor has afforded a licensee an opportunity to review standard terms, which include prominent display of the location at which the licensee can obtain the terms).

16. The UCC, which applies to contracts for the sale of goods, codifies unconscionability in § 2-302. The Restatement (Second) of Contracts sets forth its doctrine of unconscionability in § 208.

17. JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE § 4-7, at 168 (5th ed. 2000) ("Most courts take a 'balancing' approach to the unconscionability question, and to tip the scales in favor of unconscionability, most courts seem to require a certain quantum of procedural, plus a certain quantum of substantive unconscionability.").

18. Casamiquela, *supra* note 10, at 488.

> Courts are unlikely to find an online license procedurally unconscionable. If the court finds consumer assent to the license as a whole, the website provided sufficient notice to the consumer. In short, the procedural or presentational characteristics of the website are reasonable. If the court then strikes terms for reasons of procedural unconscionability, the court would contradict its initial finding of sufficient notice and consumer assent.

Id.

19. WHITE & SUMMERS, *supra* note 17, § 4-3, at 156-57.

20. RESTATEMENT (SECOND) OF CONTRACTS § 208, cmt. d (2002) ("A bargain is not unconscionable merely because the parties to it are unequal in bargaining position, nor even because the inequality results in an allocation of risks to the weaker party."); U.C.C. § 2-302, cmt. 1 (2002) ("The principle is one of the prevention of oppression and unfair surprise . . . and not of disturbance of allocation of risks because of superior bargaining power.").

guile."[21] However, at least one court has stated, "[a] contract or clause is procedurally unconscionable if it is a contract of adhesion . . . [and] a claim of procedural unconscionability cannot be defeated merely by '*any* showing of competition in the marketplace as to the desired goods and services.'"[22] In such jurisdictions, most clickwraps and browsewraps risk a finding of procedural unconscionability particularly if others do not offer a substitute product with more favorable terms.

Some courts will find unconscionability in the absence of procedural irregularities if the term at issue is substantively objectionable.[23] Whether a term limiting access to or rights in information is substantively objectionable, however, depends on a relatively sophisticated analysis of copyright law. In other words, a court cannot avoid copyright policy and a preemption analysis in assessing substantive unconscionability. Indeed, in such cases, the unconscionability and preemption inquiries may be practically inseparable.[24]

B. What Copyright Law Would Say

Copyright law generally does not preempt the terms of private contracts. Under § 301 of the Copyright Act, courts employ a two-prong test for preemption, examining (1) whether the subject matter at issue is within the scope of copyrightable subject matter; and (2) whether the right(s) at issue is (are) equivalent to those that copyright law grants.[25] If a claim meets both prongs of the test, the Copyright Act preempts it. Copyright law generally does not preempt breach of contract claims because, unlike actions for copyright infringement, they involve the extra elements of mutual assent and consideration.[26] Because the current

21. WHITE & SUMMERS, *supra* note 17, § 4-3, at 157-58 (noting that many cases involve uneducated and poor consumers, and cautioning courts against finding unconscionability simply because a consumer lacks bargaining power).

22. Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1172-73 (N.D. Cal. 2002) (emphasis in original).

23. WHITE & SUMMERS, *supra* note 17, § 4-7, at 168.

24. Note, however, that a term may be conscionable but copyright law may nevertheless preempt its enforcement. For example, if a contract forbade copying a copyrighted work, copyright law would likely preempt a breach of contract claim premised on violation of the anti-copying provision. Such a claim is not "qualitatively different" from a copyright claim based on infringement of the exclusive right of reproduction contained in §106(1) of the Copyright Act. *See, e.g.*, Nat'l Car Rental Sys., Inc. v. Computer Assocs. Int'l. Inc., 991 F.2d 426, 434 n.6 (8th Cir. 1993) (not deciding the issue but citing other courts holding a breach of contract claim preempted when "the act claimed to breach the contract involve[s] one of the exclusive copyright rights"), *cert. denied*, 510 U.S. 861 (1993); *see also infra* notes 25-26 and accompanying text (discussing preemption in more detail).

25. "[A]ll legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . and come within the subject matter of copyright . . . are governed exclusively by this title." 17 U.S.C. § 301(a) (2000).

26. Bowers v. Baystate Techs., Inc., 302 F.3d 1334, 1342 (Fed. Cir. 2002) (stating that "most courts to examine this issue have found that the Copyright Act does not preempt contractual constraints on copyrighted articles . . . In *ProCD*, for example, the court found that the mutual assent and consideration required for a contract claim render that claim qualitatively different from copyright infringement"). In *Kabehie v. Zoland*, the California Court of Appeals nicely summarized judicial

Copyright Act went into effect on January 1, 1978, most courts have conducted their preemption analyses solely under § 301 of the Act. However, the Act may impliedly preempt a cause of action that passes § 301 scrutiny if it conflicts with the statute's underlying purposes.

Consider two hypotheticals. In Hypothetical 1, A markets a software product that licensees obtain by downloading from the Internet. To obtain access to the software, the licensee must agree to a clickwrap contract that prohibits reverse engineering. B clicks on the agreement and obtains the software. B reverse engineers the software to obtain uncopyrighted information which B uses to produce an independently created, non-infringing program. A sues B for breach of the contractual obligation not to reverse engineer. What is the result?

In Hypothetical 2, C spends time and money amassing unprotected factual information, like names and addresses of restaurants in Boston. C markets the information on the Internet with a clickwrap conditioning access on the recipient's promise not to use the names and addresses for a commercial purpose. D clicks through, downloads the data, copies it, adds names and addresses of restaurants in the Boston suburbs of Brookline, Cambridge, and Newton, and markets its product in competition with C. C sues D for breach of the contractual obligation not to use the data for a commercial purpose. What is the result?

A contracts or law and economics scholar would, at first glance, find the answers easy. Both A and C should be able to recover. The clickwrap forms a contract and provisions prohibiting reverse engineering or restricting the use of data to non-commercial purposes are not unconsionable. Indeed, it's quite the opposite: most who desire the information would neither expect nor want to pay for more extensive rights.[27]

An intellectual property scholar, however, might take a different view, particularly in Hypothetical 1. Copyright law's fair use doctrine

---

approaches to preemption. 125 Cal. Rptr.2d 721 (Cal. Ct. App. 2002). As the court described, there are generally two schools of thought:

> One approach is that breach of contract actions are never preempted. This approach is based on the theory that a breach of contract includes a promise and the existence of the promise is the extra element avoiding preemption .... A second approach is a fact-specific analysis of the particular promise alleged to have been breached and the particular right alleged to have been violated.

Id. at 728.

The court adopted the second approach, stating:

> The mere breach of the promise inherent in every contract does not constitute the requisite extra element unless the promise creates a right qualitatively different from copyright. A right that is qualitatively different from copyright includes a right to payment, a right to royalties, or any other independent covenant .... If, however, the promise is equivalent to copyright, the breach of the promise is not the extra element making the action qualitatively different from copyright. In such a case, there is simply no consideration for the promise.

Id. at 734.

27. *See* White, *supra* note 6, at 1726-27 (noting that most users would not object to provisions against reverse engineering and arguing for their enforceability). *Cf.* Hillman & Rachlinksi, *supra* note 7, at 480-81 (labeling defendants who breached a clause prohibiting commercial use unsympathetic).

permits reverse engineering under certain circumstances, including those posed in Hypothetical 1.[28] Thus, the contractual provision against reverse engineering gives the copyright owner greater rights than copyright law. Should courts hold such provisions preempted to vindicate copyright policy?

As I have previously argued, for a number of reasons, courts should generally start with the proposition that fair use is an alienable right.[29] Information providers require some degree of certainty about which uses will generate revenue and which will not. Only then can they build a business case for marketing a product. But whether a particular use is fair (and thus uncompensated) is often determined only after a full trial on the merits – far after a firm must make the assumptions that support the business decision to begin production. Rather than risk having a particular use branded as fair, information providers seek to delineate specifically permitted uses: rarely do they require the purchaser to literally agree not to make fair use of material.

At the same time, however, purchasers may have legitimate expectations regarding permissible uses frustrated by boilerplate terms that effectively limit their fair use rights. Purchasers may reasonably expect the price they pay to include certain uses, particularly those that have long been permitted and customarily accepted as fair. Further, copyright policy alone might sometimes support non-enforcement of provisions barring uses that a court finds fair.

In evaluating whether a particular term limiting fair use rights should be preempted, courts should first look to the contract. They should be more willing to hold preempted inconspicuous terms that are inconsistent with reasonable expectations. Indeed, such terms may not be enforceable under contract law, obviating the need for a preemption inquiry. They should also determine whether the term is reasonable by considering its purpose and the nature of the market in which the

---

28. *See* Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527-28 (9th Cir. 1992) ("We conclude that where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law."); Atari Games Corp. v. Nintendo of Am., Inc., 975 F.2d 832, 842 (Fed. Cir. 1992) ("The Copyright Act permits an individual in rightful possession of a copy of a work to undertake necessary efforts to understand the work's ideas, processes, and methods of operation. This permission appears in the fair use exception to copyright exclusivity."). Both *Sega* and *Atari* involved reverse engineering a video game console and game cartridges to produce game cartridges. Fair use also permits reverse engineering to create a competing console. *See* Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000) (upholding reverse engineering of a game console to permit a PC to run game cartridges as a fair use). Arguably the court's holding in *Sony* is incorrect at least in the sense that it did not consider incentive effects. It would indeed be ironic if the law were to provide more protection to uncopyrighted data under the misappropriation doctrine of the *NBA v. Motorola, Inc.* case discussed *infra* note 34 than to copyrighted data under the fair use doctrine. Detailed analysis of this question is, however, beyond the scope of this paper.

29. Maureen A. O'Rourke, *Fencing Cyberspace: Drawing Borders in a Virtual World*, 82 MINN. L. REV. 609, 694 (1998).

copyrighted work competes.[30] Generally, courts should preempt only unreasonable terms. They may do so either under § 301, by holding that there is no true assent to or consideration for an unreasonable term (an approach that essentially collapses the contract and preemption inquiries into one), or impliedly under the statutory framework. Courts may also preempt otherwise acceptable terms when Congress has clearly expressed an overriding copyright policy or when a longstanding custom exists which permits a particular use.

How would the reverse engineering prohibition in Hypothetical 1 fare under such an analysis? Many likely either expect the provision or have no interest in reverse engineering. Unless the software provider has market power that leads the court to question whether the provision functions to exclude competitors, the term is likely reasonable. However, copyright policy may lead a court to preempt its enforcement. A norm has developed that permits reverse engineering under limited circumstances. That norm finds expression in commercial conduct, court cases, and legislation. Congress, in enacting the DMCA, provided an exemption from liability for circumventing access control measures to engage in reverse engineering under circumstances in which the copyright law would permit it.[31] Even the drafters of UCITA, not known for their solicitude for users of copyrighted information, agreed to include a provision refusing to enforce contractual terms prohibiting reverse engineering under similar circumstances.[32] Thus, a court might find that longstanding custom and legislative policy show a strong copyright policy supporting a refusal to enforce the term.

Hypothetical 2 involves a different problem – that of parties creating copyright rights by contract when the copyright law refuses to provide such rights. Nevertheless, an inquiry similar to that discussed above is appropriate.[33] A court's examination should consider whether the term is reasonable, keeping in mind that the information involved is uncopyrighted. In determining reasonableness, a court would consider the purpose for which the user copied the information, including whether the copier deployed it in direct competition with the original supplier, the amount taken, and the effect on the value of the original work.[34] As in

30. *See id.*

31. 17 U.S.C. § 1201(f) (2000).

32. *See* Uniform Computer Information Transactions Act § 118 (2001).

33. Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 626-27 (2001) (labeling the analysis a "reverse fair use" inquiry).

34. *Id.* Note that an alternative approach would be simply to examine the factors identified by the Second Circuit in *NBA v. Motorola, Inc.*, 105 F.3d 841 (2d Cir. 1997). There, the court held that a misappropriation claim survives a copyright preemption challenge when:

> (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 the plaintiff or others would so reduce the

the algorithm above, a court would also consider whether some overriding customary use exists that supports non-enforcement of the contractual restriction.

Under this analysis, copyright law would likely not preempt the use limitation in the contract involved in Hypothetical 2. D has taken all of the information that C gathered to compete directly with it, decreasing the value of C's product to something close to zero. The restriction, in context, is reasonable. Further, no custom exists making copying of such data to market in competition socially acceptable. Although the Copyright Act and cases interpreting it recognize a policy supporting broad availability of uncopyrighted information, in this case, another consideration consonant with copyright law – maintaining incentives to gather and disseminate information – counsels against preemption of the contractual term.

In any preemption analysis, the key point for courts to recognize is that access and use of copyrighted information are governed increasingly by standard form contracts that bind all who seek to use the information. No longer may the law distinguish between contract and copyright by stating that while contractual obligations only affect the parties to them, copyright operates against the world. Contracts have now begun to operate against the world. Courts thus need to develop modes of preemption analysis that reflect this reality and uphold copyright policy while not unduly undercutting the expectation that reasonable contractual provisions will be enforced. Here, I have pointed out that implied preemption survived the enactment of § 301 and have also suggested some guidelines to help the courts create an algorithm of analysis: assess the term's reasonableness and also consider whether custom and expectations support permitting the defendant's use despite the contractual restriction.

III. TRESPASS TO CHATTELS AND COPYRIGHT POLICY

In some cases, Internet sites do not use contractual or technological devices to regulate access; in others, they use one or both. In all of these situations, if a claim for breach of contract or violation of the DMCA fails or is otherwise unavailable, site owners may fall back on a seldom-used common law tort that has been given new life on the Internet: trespass to chattels. As I have argued at length elsewhere, some courts have mutated the traditional trespass to chattels tort into a strict liability

---

incentive to produce the product or service that its existence or quality would be substantially threatened.

Id. at 845. A court might hold that a contractual provision limiting the use of uncopyrighted data is preempted unless the defendant has breached the contract by misappropriating the information in an *NBA* sense. The virtue of the test I propose is that it is somewhat more flexible.

regime that allows Web site owners to enjoin harmless intrusions.[35] Thus, a site can keep out comparison shoppers, critics, and anyone else it does not like for whatever reason, regardless of whether or not the unwanted visitor imposes any burden on the site's servers and of whether the information extracted is copyrighted or not.

At first glance, this may seem quite sensible. The site is like private property, and a visit to the site crosses the boundary of that property. In the "real" world, property owners have strong rights to exclude for a number of policy reasons. Market forces usually push owners of private businesses to permit the efficient level of access. After all, why would any profit-maximizing business turn people away? Profit-seeking entities populate the Internet, so why shouldn't courts adopt the same system of strong property rights to regulate it?

Perhaps another hypothetical – Hypothetical 3 – will illustrate why courts should think carefully before simply replicating rights created in the "real" world on the Internet. Say that a number of local grocers operate Web sites that list products and prices. These sites are openly accessible; they do not ask users to click on any particular terms of access or use. B sets up a comparison shopping site so that customers can easily identify which store has the cheapest price for each product they wish to purchase. B obtains the pricing data by sending an automated search agent to each grocer's site to obtain the relevant information. The higher-priced grocers are less than thrilled by B's activity. They cannot stop it under contract law because B has not clicked on a contract; they cannot enjoin it under copyright law because B has not reproduced copyrightable information. Should they be able to enjoin it under a trespass theory?

At least some courts considering the issue would say "yes."[36] Assume a grocer objects to the software agent's intrusion.[37] Any further "contact" with the site by B's software agent is unauthorized, remains

35. O'Rourke, *supra* note 33. For the seminal analysis, see Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27 (2000).

36. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (upholding a trespass to chattels claim against a comparison shopping site that gathered product and pricing data by using software that searched other sites); Register.com v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (adopting the *eBay* court's approach and finding trespass to chattels when a site sent software to another to obtain names and contact information); *see also* Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH(BQRx), 2000 U.S. Dist. LEXIS 12987, at *15-16 (C.D. Cal. Aug. 10, 2000) (unpublished minute order) (accepting the *eBay* court's reasoning generally but finding no violation in the case before it because Ticketmaster could not show harm).

37. This objection is not a necessary to state a trespass claim. "A trespass to a chattel may be committed by intentionally . . . using or intermeddling with a chattel in the possession of another." RESTATEMENT (SECOND) OF TORTS § 217 (1965). The requisite intent "is present when an act is done for the purpose of using . . . a chattel. It is not necessary that the actor should know or have reason to know that such intermeddling is a violation of the possessory rights of another." *Id.* at cmt. c. As a practical matter, however, the cases generally involve some objection by the site owner. Also, interestingly, the *Register.com* court implied that the conduct at issue was not a trespass until the defendant was on notice of the plaintiff's objections to its means of access. *See* O'Rourke, *supra* note 33, at 597-98.

intentional, and continues to use some percentage of the grocer's system's resources. The grocer may show injury because even B's minimal use of its system forecloses use by others. Further, should many engage in B's activity, however unlikely that may be, their cumulative use may cause the grocer's system to crash. Thus, B has committed the cyberspace equivalent of trespass to chattels: an unauthorized use or intermeddling with the use of a chattel that causes harm.

However, this cyberspace trespass stretches the trespass to chattels cause of action to its breaking point. Traditional law requires that to recover in a cause of action for trespass to chattels, the plaintiff must show harm or deprivation of use for a substantial time. In the cases finding trespass to chattels, the courts have found neither: no evidence revealed any service disruption nor did it show that other, desired queries went unanswered or even experienced a delay in processing.[38] The courts essentially mixed and matched elements of the torts of real property trespass and trespass to chattels to create a new tort that finds liability for any unwanted, harmless intrusion.

This new trespass tort impermissibly ignores copyright policy. Access to a server necessarily causes copying of the data resident thereon. The Copyright Act, of course, provides for the exclusive right of reproduction, but that right intentionally does not extend to uncopyrighted information, including factual data like that involved in Hypothetical 3. In considering whether another non-copyright cause of action should essentially police the copying of factual, unprotected information, a court must address copyright policy and conduct a preemption analysis.

Analyzing the preemption claim under § 301, one court stated that "[t]he right to exclude others from using physical personal property is not equivalent to any rights protected by copyright and therefore constitutes an extra element that makes trespass qualitatively different from a copyright infringement claim."[39] This seems a plausible interpretation of § 301. Copyright law does not generally provide rights governing access to the physical medium on which information resides.

However, § 301 is just the starting point. An implied preemption analysis may lead to a different conclusion. Two quotes from another court at different points in time illustrate the competing interests. The court initially addressed a claim framed as trespass to a Web site, stating:

> The essence of [the] claim is the invasion and taking of factual information. . . . To the extent that state law would allow protection of factual data . . . this cannot be squared with the Copyright Act.

38. *eBay*, 100 F. Supp. 2d at 1064-66; *Register.com*, 126 F. Supp. 2d at 249-50.
39. *eBay*, 100 F. Supp. 2d at 1072.

> In addition, it is hard to see how entering a publicly available web site could be called a trespass, since all are invited to enter.[40]

In a later decision, however, that same court noted, "[i]f . . . electronic impulses can do damage to the computer or to its function in a comparable way to taking a hammer to a piece of machinery, then it is no stretch to recognize that damage as trespass to chattels and provide a legal remedy for it."[41] Thus, there are two sides to the equation: copyright policy supports broad access to factual information but other law may seek to define the permissible *means* of access. How should courts reconcile these two concerns?

I have argued elsewhere that courts addressing access to publicly available Web sites should employ a nuisance/misappropriation model that might be augmented by safe harbor rules to enhance certainty.[42] For example, courts could consider how much of a burden unwanted access places on system resources. The law might also impose a duty of reasonable care on those who access Web sites by setting standards for what burden on system resources from a single source is reasonable, and finding liability when a site visitor exceeds that level. When the claim is based not on the means of access, but rather on what the user does with the information once obtained, courts should evaluate the claim under copyright law as supplemented by state misappropriation law. Copyright law simply cannot abide a tort of trespass to information itself. The approach I suggest reconciles copyright policy with concerns about access that imposes an unusual burden.

The same concerns that animated the discussion of contract law above are re-created in the trespass context. In a sense, trespass law functions like an implied contract regulating terms of access. However, when courts apply trespass law to access to information rather than real property or chattels, they should do so with regard for copyright policy and adjust the cause of action accordingly. The cost/benefit analysis that supports extensive property rights in the "real" world may be different in cyberspace, calling for a nuanced analysis.

IV. THE COMPUTER FRAUD AND ABUSE ACT AND COPYRIGHT POLICY

The preceding discussion of state law causes of action may become irrelevant if Web site owners continue to turn to federal legislation in the form of the Computer Fraud and Abuse Act ("CFAA") to protect against unwanted access. Indeed, the CFAA may prove more useful to Web site owners than state law causes of action simply because it is a

40. Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654 HLH(BQRx), 2000 U.S. Dist. LEXIS 4553, at *10-11 (C.D. Cal. Mar. 27, 2000) (citations omitted). The court referred to § 301 in its opening but also implied that principles other than § 301 supported the proposition that "where copying is permitted by the Copyright Act, a contrary state law could not be enforced." *Id.*

41. *Ticketmaster Corp.*, 2000 U.S. Dist. LEXIS 12987, at *16.

42. O'Rourke, *supra* note 33, at 620-29 (discussing the approach mentioned in the text in detail).

federal law and thus on an equal footing with copyright law; courts are much more likely to find that copyright policy "preempts" a state law than another federal statute. Interestingly, though, Congress enacted the CFAA to address problems of computer crime, focusing on theft of confidential information.[43] Congress likely did not intend the statute to become the potent weapon that it now is "against employees, former employees, competitors and others."[44] Unanticipated uses of the Act have arisen because its language is not limited to cases of hacking but instead is broad enough to encompass a wide range of conduct.

The CFAA essentially functions like a federal claim for trespass.[45] A person violates the CFAA when, for example, he or she "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information"[46] or "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes loss."[47] Generally, to maintain a civil action, the plaintiff must prove a minimum loss of $5,000 in addition to proving a violation of one of the Act's substantive provisions.[48] The Act defines "damage" as "any impairment to the integrity or availability of data, a program, a system or information;"[49] it defines "loss" as:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[50]

Consider Hypothetical 3 again. A grocer's site may object to B's access, post a notice forbidding access like B's, or require B as a condition of access to click on a contract that forbids using automated tools to access the site and/or using information obtained from the site

---

43. For an excellent history of the CFAA, see Christine D. Galbraith, Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites 13-19 (Sept. 20, 2002) (unpublished manuscript, on file with author).

44. Michael R. Levinson & Christopher E. Paetsch, *The Computer Fraud and Abuse Act: A Powerful New Way to Protect Information*, 19 THE COMPUTER & INTERNET LAWYER, at 11 (2002); *see also* Galbraith, *supra* note 43, at 19 ("Noticeably absent from the legislative history ... is any suggestion that Congress intended to drastically widen the protection of the CFAA to include all information and all computer systems on the Internet ....").

45. However, plaintiffs will likely find it easier to succeed on a CFAA claim than one for trespass. The CFAA is a federal law on par with copyright, and therefore runs less risk of preemption. Also, although some courts do not require harm as a condition of showing trespass to chattels on the Internet, others may, and plaintiffs may have some difficulty showing harm. The CFAA generally requires showing only "loss," a much easier standard to meet. *See* Galbraith, *supra* note 43, at 30-31; *infra* notes 48-50 and accompanying text.

46. 18 U.S.C. § 1030(a)(2)(C) (2000).

47. *Id.* § 1030(a)(5)(A)(iii). To violate this clause, the access must also generally cause loss or physical injury, impair medical treatment, or threaten public health or safety. *Id.* § 1030(a)(5)(B).

48. *Id.* § 1030(g). If the substantive violation is one that requires damage, the plaintiff would, of course, have to show damage in addition to loss. *Id.* §§ 1030(a)(5)(A)(i) – (a)(5)(B)(v).

49. *Id.* § 1030(e)(8).

50. *Id.* § 1030(e)(11).

for commercial purposes.[51] Does B violate the CFAA under any of these scenarios by using an automated tool to obtain product and pricing information that it then uses for a commercial purpose – to attract visitors to her own comparison shopping site?

She certainly has intentionally accessed the computer. If the grocer is entitled to object to her access (say, under trespass law) or the notice or contract is binding, then her access is without authorization. This, of course, highlights the importance of the copyright preemption inquiry. That analysis will likely decide whether or not the site's objection, notice, and/or contract are, in fact, binding. If they are, she has likely violated the CFAA if the site can show $5,000 in loss. The site can probably do so quite easily. It should simply spend $5,000 on consultants who determine whether B's activity corrupted any data.

B might also be liable for exceeding her authorized access because she obtained the data knowing that she would breach the contractual restriction prohibiting commercial use. According to at least one court, such conduct violates the CFAA:

> [N]either party disputes that [the defendant] is not authorized under [the plaintiff's] terms of use to use the data for mass marketing purposes, and neither party disputes that [the defendant] is authorized to obtain the data for some purposes .... [However], the means of access [the defendant] employs... is unauthorized. Second, even if [defendant's] means of access ... would otherwise be authorized, that access would be rendered unauthorized *ab initio* [because] prior to entry [the defendant] knows that the data obtained will be later used for an unauthorized purpose.[52]

This holding is arguably wrong as a matter of statutory interpretation and almost certainly wrong from a policy perspective. The statute defines "exceed[ing] authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter."[53] These words do not refer to what the accessor does with the information that he is entitled to obtain nor should courts stretch them to regulate use. Copyright law is best suited to evaluating whether a particular use of information violates one of the exclusive rights of the copyright owner or a non-preempted contractual restriction. Certainly, it seems excessive to threaten garden-variety commercial and/or consumer concerns with civil liability and the criminal sanctions that the CFAA provides for engaging in conduct that may not even be copyright infringement. If copyright infringement occurs, the Copyright Act rather

51. *See* Galbraith, *supra* note 43, at 41 (discussing ways in which Web site owners attempt to regulate access, and giving contracts, technological measures, and direct communication as examples).

52. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000).

53. 18 U.S.C. § 1030(e)(6).

than the CFAA provides the appropriate standards for liability, including criminal penalties.

Ultimately, Congress should refine the CFAA to limit parties' abilities to sue for unauthorized access and exceeding authorized access to align the statutory wording with the limited legislative intent.[54] Courts, in the meantime, should be wary of imposing liability under the CFAA for access to a publicly available Web site. In particular, they should make use of preemption analysis and not interpret the statute to encompass situations that do not literally fall within its terms.

V. CONCLUSION

Unfettered private ordering of the Internet through contract and expansive property rights would likely produce an Internet very different from the one to which we have been accustomed. Such private ordering also implicates the concerns of copyright law which include facilitating both the production and dissemination of information. Both Congress and the courts will increasingly confront issues requiring them to make difficult decisions about permissible conduct on the Internet. Whatever algorithm they use to make policy choices, it must include consideration of copyright policy.

54. *See* Galbraith, *supra* note 43, at 67-69 (proposing amendments that would eliminate the ability to bring a civil action based on access and copying of information provided on a publicly available Web site).