DEFENDING CYBERPROPERTY

PATRICIA L. BELLIA*

In this Article, Professor Patricia Bellia explores how the law should treat legal claims by owners of Internet-connected computer systems to enjoin unwanted uses of their systems. Over the last few years, this question has become increasingly urgent and controversial, as system owners have sought protection from unsolicited commercial e-mail and from "robots" that extract data from Web servers for competitive purposes. In the late 1990s and early 2000s, courts utilizing a wide range of legal doctrines upheld claims by network resource owners to prevent unwanted access to their computer networks. The vast weight of legal scholarship has voiced strong opposition to these "cyberproperty" claims, arguing that such property-rule protection would threaten productive uses of the Internet, inhibit innovation, or even create an anticommons.

This Article challenges the typical criticisms of property-rule protection, demonstrating that they are based on simplifications or false assumptions about the behavior of system owners and the nature of the Internet. Most importantly, scholars have overlooked the use of technical measures to block access, in conjunction with or in place of legal measures. The Article then lays out a wide range of potential legal rules for network resources, from absolute property-rule protection to a "technology displacing" approach that actually limits the technical barriers a system owner can impose, with a number of "loperty" rules—involving property-rule protection triggered by a system owner taking a particular measure—in between. After examining the existing case law, the Article agrees that courts' recent trend toward a closed-access property-rule regime is inappropriate. Professor Bellia, however, demonstrates that attempts to preserve open access by rejecting any sort of property-rule protection are equally misguided. She points out that too-weak legal protection will prompt greater reliance on technical measures that mimic a property-rule approach, similarly limiting access. Yet, because technology lacks the flexibility and common sense exceptions inherent to legal application, the results for the community-at-large could be worse.

The Article concludes that entitling a system owner to property-rule protection so long as she provides the user with actual notice of permissible uses of the system or adopts a system configuration making it plain to the user that access is restricted would better balance the interests of consumers and system owners than rejecting property-rule protection outright. Although such an approach might be inappropriate in a limited class of cases—as, for example, when a system owner's predominant motive for limiting access is anticompetitive in nature—Professor Bellia demonstrates that courts and legislatures can apply technology-displacing measures in such cases to achieve an appropriate legal balance.

INTRODUCTION 2166
I. THE CYBERPROPERTY CONTROVERSY 2174

 Associate Professor of Law, Notre Dame Law School. A.B., Harvard College, J.D., Yale Law School. I thank A.J. Bellia, Paul Schiff Berman, Nicole Garnett, Orin Kerr, David McGowan, Mark Movsesian, John Nagle, David Post, Jack Pratt, Bob Rodes, and Jay Tidmarsh for helpful discussions. Gretchen Heinze provided excellent research assistance.

A. *The Evolution of Electronic Trespass Doctrine* 2175
B. *The Harm-Based Doctrinal Critique and Its Challenges* 2178
C. *Normative Critiques* 2189
1. *The Competing Interests in Cyberproperty Claims* 2191
2. *"Overpropertization" Critiques and Their Limitations* 2193
a. Cyberproperty Claims as Enclosure of Intellectual Property 2194
b. Bargaining and Valuation Problems Under a Property-Rule Approach 2201
II. REGULATORY APPROACHES IN LAW AND CODE 2210
A. *Four Legal Approaches to Protecting Network Resources* 2211
B. *Variance Within and Blurring Between Legal Approaches* 2213
C. *Regulatory Effects of Law and Code* 2218
D. *Property and Liability Rules Revisited* 2220
III. RETHINKING CYBERPROPERTY CLAIMS 2224
A. *Current Legal Approaches* 2225
1. *Trespass to Chattels* 2226
a. Actual Notice Cases 2226
b. Policy Statements and Terms of Use 2228
c. Cases Rejecting Trespass Claims 2230
2. *The Computer Fraud and Abuse Act* 2232
a. Bulk E-Mail Cases 2234
b. Automated Query Cases 2237
3. *Contract Law* 2241
4. *Summary* 2245
B. *Curtailing the Drift Toward a Closed-Access Default* 2245
C. *The Choice Between Notice-Based, Code-Based, and Commons Approaches* 2252
1. *Doctrinal Issues: The Computer Fraud and Abuse Act* 2253
2. *Doctrinal Issues: Trespass to Chattels* 2258
3. *Normative Considerations: The Problem of Code* 2261
CONCLUSION 2272

INTRODUCTION

When can the owner of a computer system connected to the Internet assert a right to "exclude" unwanted uses of her system? Disputes typically arise in one of two contexts: when a provider of e-mail services wishes to block unsolicited commercial e-mail, or when the owner of a web server seeks to restrict how others gather and use information available on that system. Over the last several years, system owners have invoked a wide range of legal doctrines as bases for enjoining unwanted access to their systems, and courts have largely—and controversially—accepted their claims.

The earliest cases involved claims that objectionable activities—typically, the sending of large quantities of unsolicited commercial e-mail—constituted a common-law "trespass to chattels." Courts held that the e-mail provider had a possessory interest in its mail servers, that the unsolicited e-mails interfered with that interest, and that the provider was entitled to injunctive relief to block the unwanted activities.[1] Courts soon extended the trespass-to-chattels theory beyond that narrow functional context, to cases in which website operators claimed that competitors used objectionable methods, such as automated queries, to extract data from their systems,[2] and then to cases in which e-mail providers sought to block relatively small numbers of unsolicited, but noncommercial, e-mail messages.[3] More recently, in

---

[1] *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–28 (S.D. Ohio 1997) (granting preliminary injunction against sending of bulk e-mail); *see also* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1279–80 (N.D. Iowa 2000) (recognizing trespass based on sending of bulk e-mail, but deferring decision on issue of corporation's liability for harms caused by individual e-mailer); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 897–98 (N.D. Iowa 2001) (finding corporation liable for actions of individual e-mailer and awarding damages for trespass); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998) (granting permanent injunction against sending of bulk e-mail); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–52 (E.D. Va. 1998) (granting summary judgment on claim that bulk e-mailer was liable for trespass but deferring determination of damages to trial). A variant on this claim involves the use of an account with a particular Internet service provider (ISP) to send unsolicited e-mail, which results in the ISP being overwhelmed with misdirected replies. *See* Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020, 1025 (N.D. Cal. 1998).

[2] *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–72 (N.D. Cal. 2000) (granting preliminary injunction against use of automated software to gather data from auction pages); *see also* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 396, 404 (2d Cir. 2004) (affirming preliminary injunction against use of automated software to extract information about new domain-name registrants from public database for solicitation purposes); Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724, 2001 WL 1736382, at *11–*13 (N.D. Cal. Dec. 6, 2001) (declining to dismiss trespass claim based on use of automated software to copy codes from plaintiff's website).

[3] *See* Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 246–47 (Ct. App. 2001), *rev'd*, 71 P.3d 296 (Cal. 2003).

addition to raising state-law trespass claims, plaintiffs seeking to prevent unwanted uses of their computer systems have brought successful civil claims under the federal Computer Fraud and Abuse Act (CFAA),[4] which in some circumstances prohibits unauthorized access to "protected" computers—a category that likely encompasses any computer linked to the Internet.[5] Plaintiffs have also invoked contract law to enforce restrictions on uses of their systems.[6] Finally, when a web server holds material entitled to copyright protection, the Digital Millennium Copyright Act (DMCA)[7] or even a straightforward copyright infringement claim may provide grounds for owners to limit access in certain cases.[8]

---

[4] 18 U.S.C.A. § 1030 (West 2000 & Supp. 2004).

[5] 18 U.S.C. § 1030(e)(2) (2000 & Supp. I 2001) (defining "protected computer" to include any computer "used in interstate or foreign commerce or communication"); *see* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–84 (1st Cir. 2001) (affirming grant of preliminary injunction under § 1030(a)(4) of Computer Fraud and Abuse Act (CFAA) against use of software program to extract tour codes and prices from website of tour company); *Nat'l Health Care Disc.*, 174 F. Supp. 2d at 898–99 (concluding that AOL member's harvesting of addresses of other AOL members for purpose of sending unsolicited commercial e-mail violated § 1030(a)(2)(C) of CFAA); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 251–52 (S.D.N.Y. 2000) (finding that use of automated queries to extract information from publicly available database violated § 1030(a)(5)(C) of CFAA), *aff'd on other grounds*, 356 F.3d 393 (2d Cir. 2004); *LCGM*, 46 F. Supp. 2d at 450–51 (holding that harvesting of e-mail addresses for purpose of sending unsolicited commercial e-mail violated § 1030(a)(2)(C) and § 1030(a)(5)(C) of the CFAA); *see also eBay*, 100 F. Supp. 2d at 1069 (noting but not deciding claim under CFAA).

[6] *See, e.g.*, *Register.com*, 356 F.3d at 398–404 (affirming grant of preliminary injunction on claim that use for solicitation purposes of information gathered from publicly available database constituted breach of contract); Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2003 WL 21406289, at *1–*2 (C.D. Cal. Mar. 7, 2003) (denying defendant's motion for summary judgment on claim that use of automated software breached contractual limitations on use of website); Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 982 (E.D. Cal. 2000) (declining to dismiss claim that use of information collected from site for commercial purposes constituted breach of contract); *Hotmail*, 47 U.S.P.Q.2d (BNA) at 1025 (finding Hotmail likely to succeed on claim that subscribers' use of Hotmail accounts to send spam and pornography violated contractual restrictions).

[7] 17 U.S.C. § 1201(a)(1)(A) (2000) (prohibiting circumvention of "a technological measure that effectively controls access to a work protected" under copyright law). The Digital Millennium Copyright Act (DMCA) would apply only if a website used technical measures to limit access. None of the cases brought thus far under the DMCA's anticircumvention provision, which took effect in October 2000, *see id.*, have involved unauthorized access to a website or similar information-serving system. I therefore do not discuss the DMCA at length. It is worth noting, however, that interpretive issues under the DMCA raise some of the same concerns that arise with respect to other cyberproperty claims. *See infra* note 143.

[8] For an example of an attempt to invoke copyright law to block the use of automated queries to extract information from a site, see *Ticketmaster*, 2003 WL 21406289, at *4–*6. The case involved Ticketmaster's claim that Tickets.com wrongfully used automated software to extract information from Ticketmaster's website. Because copyright law protects neither facts nor compilations of facts that are insufficiently original, *see* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344, 348 (1991), Ticketmaster could not claim that

Although network resource owners have largely been successful in enjoining unwanted uses of their systems, the law remains very much in flux. In a recent case that is likely to be influential, the California Supreme Court rejected a trespass-to-chattels claim brought by Intel Corporation seeking to bar its former employee, Kenneth Hamidi, from transmitting e-mail to current employees through the company's mail servers.[9] The court held that Intel could not sustain a trespass claim without showing that Hamidi's e-mails threatened to impair the functioning of Intel's mail servers.[10] While the *Hamidi* court attempted to distinguish the case law involving unsolicited commercial e-mail and the use of automated queries,[11] the case will likely have repercussions in those contexts as well. In particular, courts applying *Hamidi*'s physical-harm requirement will have difficulty declaring that objectionable activities that do not clearly

---

Tickets.com violated copyright law merely by listing Ticketmaster's information on events and ticket prices. The court thus focused on whether the temporary copying of Ticketmaster's webpages on Tickets.com's computers, so that Tickets.com could then extract the unprotected factual data, constituted copyright infringement. Analogizing to cases holding that reverse engineering of software in order to access unprotected components constitutes a fair use, the court granted Tickets.com summary judgment dismissing the copyright claim. *Ticketmaster*, 2003 WL 21406289, at *4–*5 (citing Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992)).

As other commentators have discussed, this aspect of the *Ticketmaster* court's decision was likely correct. *See, e.g.*, David Kramer & Jay Monahan, *Panel Discussion—To Bot or Not To Bot: The Implications of Spidering*, 22 HASTINGS COMM. & ENT. L.J. 241, 253 (2000) (discussing *Sega*'s implications for copyright claims challenging automated queries); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 583 & n.90 (2001) (discussing application of *Sony* and *Sega* to extraction of product and pricing information from websites). Because other copyright claims involving factual information will face similar obstacles, I do not discuss such claims at length in this Article. Of course, had Tickets.com displayed the Ticketmaster information in such a way as to capture protectable components of Ticketmaster's expression, the copyright claim would have been more complicated. *Cf.* Kelly v. Arriba Soft Corp., 280 F.3d 934, 948 (9th Cir. 2002) (holding that search engine's framed display of full-sized photographic images violated copyright law, but that reproduction of thumbnail-sized images constituted fair use), *withdrawn and superseded*, 336 F.3d 811, 822 (9th Cir. 2003) (holding that reproduction of thumbnail-sized images constituted fair use, but remanding for further consideration of whether framed display of full-sized images violated copyright law because neither party sought summary judgment on that claim).

[9] Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003). Because of the high proportion of technology businesses located in California, disputes over unwanted access are likely to arise there relatively frequently. Several trespass cases have involved application of California law. *See* Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724, 2001 WL 1736382, at *11 n.10 (N.D. Cal. Dec. 6, 2001); *eBay*, 100 F. Supp. 2d at 1072; *Hotmail*, 47 U.S.P.Q.2d (BNA) at 1023.

[10] *Hamidi*, 71 P.3d at 300.

[11] *Id.* at 304–08.

threaten the computer system itself—such as automated queries to extract data—constitute a trespass to chattels.

This Article explores how the law *should* treat a network resource owner's attempts to prevent unwanted access to her system.[12] Although the various legal doctrines that plaintiffs invoke to block unwanted uses of network computing resources are distinct, each doctrine involves the same underlying claim: that the system owner should have the right to set the terms of access to the resource, a default conventionally known as property-rule protection. Under a property-rule approach to network resources, a system owner is entitled to enjoin unwanted uses, and thus controls the terms of access. I refer to the various doctrinal routes to controlling the terms of access collectively as "cyberproperty" claims.[13] Although plaintiffs have successfully pressed cyberproperty claims in court, the weight of scholar-

[12] In casting the inquiry as how the law should treat a resource owner's attempts to prevent unwanted uses of her *system*, I do not intend to obscure the fact that, in a significant number of cases, blocking unwanted uses of a system is equivalent to controlling the acquisition and use of information. *See infra* notes 108–10 and accompanying text. There is significant recent literature pointing out how characterizing a claim as involving access to a "system" versus access to "information" can profoundly influence how courts resolve the claim. *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 502 (2003) (arguing that courts' focus on cyberspace as "a place" has led courts to recognize private property rights too readily); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 529 (2003) (arguing that courts treating websites as analogous to real property have ignored that disputes over access to systems "were really efforts to control the flow of information to or from a site"); Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 244–45 (2003) ("Many instances of complaints about unauthorized access to a *computer system* are really premised on the complainant's concerns about unauthorized access to and/or use of data stored within the system."); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 434–45 (2003) (discussing "Internet-as-place" metaphor and concluding that it has "captured the imagination of legislators and judges . . . for whom a rule of 'exclusion-from-computer' naturally assumes a rule of 'exclusion-from-information'"); O'Rourke, *supra* note 8, at 580 (observing that courts considering claims to exclude unwanted uses emphasize "different factors depending on whether they focus on the website . . . or the tangible server"); *see also* Brett M. Frischmann, *The Prospect of Reconciling Internet and Cyberspace*, 35 LOY. U. CHI. L.J. 205, 205 (2003) (discussing scholars' observations that "the outcome of many cyberlaw disputes depends significantly, if not entirely, on a judge's perspective of the Internet and how it works"). I do address at length the consequences that allowing a resource owner to control uses of her system can have for information policy. *See infra* notes 120–53 and accompanying text. I use the "unwanted uses of her system" label simply to capture cases that involve mail servers, as well as cases that involve web servers.

[13] In describing claims that network resource owners should be able to dictate the terms of access to their systems as "cyberproperty" claims, I am adopting a somewhat narrower usage of that term than do other scholars. *See, e.g.*, Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 MINN. L. REV. 129, 146–47 (1998) (using "cyberproperty" to describe recognition of entitlements in cyberspace, without specifying whether those entitlements would entail property-rule or liability-rule protection).

ship opposes such claims in favor of a liability-rule approach to protecting network resources.[14] Under a liability-rule approach, access is permitted, subject to terms set by a third party, typically a court or legislature.

This Article argues that property-rule protection for network resources is more appropriate than scholars have thus far recognized. Commentators favor liability-rule protection for network resources[15] in part based on a fear that granting system owners the right to exclude unwanted uses will have disastrous consequences for the development and growth of the Internet.[16] That view rests on two

---

My cross-doctrinal approach to cyberproperty claims is not unique; notable works include Madison, *supra* note 12, and a series of pieces by Maureen A. O'Rourke, *see* Maureen A. O'Rourke, *Common Law and Statutory Restrictions on Access: Contract, Trespass, and the Computer Fraud and Abuse Act*, 2002 U. ILL. J.L. TECH. & POL'Y 295 [hereinafter O'Rourke, *Restrictions on Access*]; O'Rourke, *supra* note 8; 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*]. As will become clear, however, my analysis differs from Madison's and O'Rourke's in important respects.

[14] *See, e.g.*, Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53 (2000) (favoring "nuisance" approach to website access, under which courts would weigh whether "the cost of the intrusive activity outweighs the benefit"); Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 629 (2004) (suggesting application of existing nuisance doctrine); O'Rourke, *Shaping Competition*, *supra* note 13, at 2001–03 (proposing balancing test analogous to nuisance); Steven Kam, Note, Intel Corp. v. Hamidi*: Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427, 448–52 (2004) (advocating "cyber-nuisance" approach); *see also* Symposium, *The Internet: Place, Property, or Thing—All or None of the Above?*, 55 MERCER L. REV. 867, 912 (2004) (comments of Jennifer Stisa Granick, favoring nuisance approach over recognition of right to exclude). For related critiques of courts' approach, see sources cited *infra* note 59. For defenses of a property-rule approach, see Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 84 (2003) ("[S]trong property rights for non-network elements function as well in cyberspace as they do anywhere else."); David McGowan, *Website Access: The Case for Consent*, 35 LOY. U. CHI. L.J. 341, 375–83 (2003) (explaining benefits of property-rule approach over damages rule such as nuisance).

[15] I later argue that the traditional property rule/liability rule framework does not adequately capture the range of possible legal rules for protection of network resources. *See infra* Part II.A. In particular, even those scholars who oppose recognition of a system owner's right to exclude unwanted uses seem to acknowledge that the system owner should be able to enjoin evasions of very strong technical measures, such as password protection. *See infra* notes 155–57 and accompanying text. Characterizing these scholars as favoring "liability" rule protection is therefore somewhat imprecise because they would allow injunctive relief to back the terms of access the system owner sets through technical measures, independent of any showing of a threat of harm. The point for now is that the scholars whose arguments I challenge favor recognition of a right to exclude in an extremely narrow category of cases, if at all.

[16] *See, e.g.*, Brief of Amici Curiae Mark A. Lemley et al. in Support of Bidder's Edge, Appellant, Supporting Reversal at 8 & n.7, 9–10, eBay, Inc. v. Bidder's Edge, Inc., No. 00-15995 (9th Cir. submitted June 22, 2000) (arguing that right to exclude threatens to make search engines and linking illegal); Brief of Amici Curiae Professors of Intellectual Property and Computer Law, Supporting Reversal at 10–12, Intel Corp. v. Hamidi, 71 P.3d 296

further premises. First, commentators fear that system owners will exercise the right to exclude unwanted uses too frequently, blocking many harmless and productive activities. Indeed, some scholars seem to treat property-rule protection of network resources as equivalent to setting a default rule of closed access, with would-be users required to bargain for any and all access, regardless of a system's technical configuration.[17] Second, commentators assume that liability-rule protection for network resources will be sufficient to preserve open access to network resources.

As I will argue, however, the view that liability-rule protection will lead to a greater degree of open access than property-rule protection is questionable. First, although a property-rule approach has prevailed in many contexts, scholars' dire predictions about the effects of such an approach on the shape of the Internet have not come to pass.[18] That is no doubt in part because a default rule of closed access is not an inevitable result of a property-rule approach. Eliminating the closed-access-default assumption blunts the force of the criticism of a property rule. Second, it is not clear that a liability approach will lead to open access. In the absence of property-rule protection, system owners can deploy technical measures of varying strength in an effort to achieve the desired level of control. Those measures need not be foolproof to affect users' access.

In other contexts, scholars have recognized the effect that technical measures will have on access to and use of information.[19] What the debate over cyberproperty claims overlooks, however, is that the choice of a particular legal rule is likely to influence the technical measures that a system owner employs. In particular, a system owner faced with weak *legal* protection of network resources can respond by employing stronger *technical* measures to control access. That possibility itself may not be troublesome because the access baseline remains the same under either approach. It quickly becomes apparent, however, that the balance between legal and technical measures matters. Commentators have suggested that the nature of technical measures makes *governmental* choices to rely on such measures rather than legal measures troubling, in large part because regulation through technical measures produces complete control not available

(Cal. 2003) (No. S103781) (same); Burk, *supra* note 14, at 49 (arguing that granting network resource owners right to exclude unwanted uses could create "anti-commons nightmare"); Hunter, *supra* note 12, at 508–09 (predicting severe constraints on search engines and disappearance of aggregation products).

[17] *See infra* pp. 2207–08.

[18] *See infra* notes 187–91 and accompanying text.

[19] *See infra* notes 133–34 and accompanying text.

through law alone.[20] Concerns of this sort apply with equal force when private parties seek to use technical rather than legal measures to control access to their systems.

If courts follow the prevailing scholarly sentiment,[21] they will reject strong legal protection for network resources. Because a property-rule approach has so often been caricatured as leading to a default rule of closed access, it seems to have few benefits to offer. The promise of open access that a liability-rule approach seems to carry, however, may well be equally illusory. Before we rush to embrace a liability-rule approach, then, we must consider both the real scope of property-rule protection and the pressure that the choice of a particular legal rule may place on the use of technical measures. This Article seeks to consider this broader range of normative arguments and argues that the liability-rule trend scholars hope to launch is ill-conceived.

The Article proceeds as follows: In Part I, I use electronic trespass cases to introduce the doctrinal and normative complexities of cyberproperty claims. In electronic trespass cases, courts initially granted property-rule protection to network resources, recognizing system owners' rights to enjoin unwanted uses and thus to set the terms of access. Scholars heavily criticized these decisions, partly on the ground that courts overlooked or misapplied the requirement that a plaintiff asserting a trespass-to-chattels claim demonstrate harm. In *Hamidi*, the California Supreme Court seized upon this critique, declaring that a trespass-to-chattels claimant could not secure injunctive relief merely by demonstrating an unwanted use of her system.[22] Although the *Hamidi* court cast its decision as a straightforward application of trespass doctrine, I show that the harm issue is difficult to resolve at the level of doctrine. I then turn to the normative issues at stake in cyberproperty claims. Scholars reject property-rule protection for network resources partly out of fear that recognizing a right to exclude unwanted uses will lead to "overpropertization" of the Internet, by curtailing the development of useful tools and diminishing the network benefits of the Internet. Although I sympathize with these concerns, I show that certain assumptions underlying scholars' arguments are unwarranted.

In Part II, I offer a framework for considering cyberproperty claims that is more nuanced than the basic property/liability framework. I first set forth four possible *legal* approaches to cyberproperty

---

[20] *See infra* notes 391–407 and accompanying text.

[21] As I later explain, the California Supreme Court recently did so in *Intel Corp. v. Hamidi*. *See infra* notes 22, 64–99 and accompanying text.

[22] *See Hamidi*, 71 P.3d at 310–11 (discussing commentators' concerns).

claims. Under three of these approaches, a system owner has a right to enjoin unwanted uses in some circumstances. In this sense, all three approaches involve property-rule protection. Only one of these three approaches, however, involves a default presumption of closed access. The remaining two approaches differ in what triggers the right to injunctive relief to back the terms of access the system owner sets: Under one approach, an appropriate form of notice to would-be users triggers the system owner's right to exclude; under another, only the use of technical measures that are actually effective in blocking some access triggers such a right. I then explore more fully the role of *technical* measures in protecting access to network resources. Technical measures can serve as a trigger for legal protection; but, even under a legal rule that denies injunctive relief for unwanted uses, system owners may independently use such measures to block some access. I argue that the availability of technical measures to block access should affect how we analyze cyberproperty claims in two ways. First, the fact that system owners can turn to technical protection when legal protection is lacking means that the absence of legal protection will not necessarily lead to open access. Second, the choice of a particular legal approach may induce greater reliance on technical measures than would be necessary with a stronger legal rule.

Part III applies the framework set forth in Part II. I first explore the cyberproperty case law. While I point out that, contrary to scholars' claims, the most important early cases do not reflect a closed-access approach under which all users must bargain for access to a system, I argue that courts' more recent drift toward closed access is both doctrinally and normatively inappropriate. That conclusion, however, does not provide a basis for choosing among the other possible approaches. I then demonstrate that courts should apply the federal Computer Fraud and Abuse Act only when a system owner uses strong technical measures to control access, and argue that courts have too broadly interpreted that statute by allowing system owners to invoke it to enforce terms of use and other weak forms of notice. With respect to other cyberproperty claims, however, the arguments for requiring technical measures to trigger a right to exclude are weaker. Turning to the normative considerations, I argue that the approaches scholars currently favor will not lead to the degree of open access they predict, for those approaches will induce greater reliance on technical measures that mimic the effect of the legal rules scholars oppose. Moreover, because technical measures raise concerns that legal measures do not, the balance between technical and legal measures matters. The law should not demand technical measures as a prerequisite to a system owner's ability to exclude unwanted uses. So

long as the law presumes a default rule of open access and places the burden on the system owner to adequately convey the limits on permissible uses of her system, property-rule protection for network resources is appropriate.

I
THE CYBERPROPERTY CONTROVERSY

Plaintiffs seeking to block unwanted uses of network computing resources have relied on a range of legal doctrines—trespass-to-chattels claims, CFAA claims, contract claims, and copyright-related claims. In this Part, focusing primarily on the tort of trespass to chattels, I introduce the doctrinal and normative complexities of these cyberproperty claims. Although the claims are doctrinally distinct, they raise the same competing interests: interests of resource owners in protecting their investments in equipment and particular business models; interests of users in open access to information and open avenues for speech; interests of society as a whole in preserving the benefits of a large-scale computer network; and, assuming some limitations on access are appropriate, interests of users in fair notice of the conditions of access. The question becomes: What sort of legal protection for network resources best balances these interests?

In Section A, I trace the evolution of electronic trespass doctrine with respect to claims involving unsolicited e-mail and the use of automated queries to gather data from websites. In Section B, I evaluate scholars' doctrinal critique of the electronic trespass cases. That critique focuses largely on the question of what harm, if any, a plaintiff must show to sustain a trespass claim, and argues that courts have ignored or misapplied the harm requirement. In *Intel Corp. v. Hamidi*, the California Supreme Court embraced this doctrinal critique, holding that an electronic trespass claim requires a showing of threatened damage to or impairment of the functioning of the plaintiff's computer equipment.[23] As I argue, however, the issue of what harm, if any, a plaintiff must show to sustain a trespass-to-chattels claim cannot be resolved at the level of doctrine. Section C thus turns to scholars' normative arguments against recognition of cyberproperty claims. I argue that scholars tend to caricature approaches that would grant system owners a right to exclude unwanted uses, and fail to identify a compelling conceptual basis for choosing among the possible approaches to protecting network resources.

---

[23] *Id.* at 300.

A. The Evolution of Electronic Trespass Doctrine

Under section 217 of the *Second Restatement of Torts*, a plaintiff asserting a trespass-to-chattels claim must demonstrate that the defendant intentionally interfered with the plaintiff's possessory interest in personal property, either by "dispossessing [the plaintiff] of the chattel" or by "using or intermeddling with" the property.[24] The tort was first applied in the Internet context in *CompuServe Inc. v. Cyber Promotions, Inc.*,[25] where CompuServe successfully argued that Cyber Promotions's transmission of unsolicited commercial e-mail to CompuServe subscribers constituted a trespass to CompuServe's mail servers. The court's reasoning on three crucial issues formed the foundation for later decisions.

The first issue was whether transmission of e-mail to a mail server could constitute use of or intermeddling with that server for purposes of the trespass tort. Relying on a California case that applied a trespass-to-chattels rationale to two teenagers' efforts to hack into a telephone system, the *CompuServe* court deemed Cyber Promotions's "contacts" with CompuServe's computer system—that is, Cyber Promotions's sending of e-mail—to be "sufficiently physically tangible to support a trespass cause of action."[26] The second issue was whether Cyber Promotions's activities were in fact unauthorized. The court rejected the argument that CompuServe, by virtue of connecting its system to the Internet and configuring it to accept incoming e-mail on behalf of its subscribers, had impliedly consented to Cyber Promotions's activities: Because CompuServe sent Cyber Promotions a cease-and-desist letter, Cyber Promotions had received specific notice that CompuServe "no longer consented" to Cyber Promotions's use of its system.[27]

The final issue was what kind of harm, if any, CompuServe needed to demonstrate to obtain an injunction on a trespass-to-chattels theory. The *Second Restatement of Torts* states that a dispossession may be actionable even in the absence of any harm, but that one is generally liable for using or intermeddling with a chattel only if the chattel's owner can demonstrate harm. In particular, according to the *Restatement*, a defendant is liable only if:

(a) he dispossesses the other of the chattel, or

(b) the chattel is impaired as to its condition, quality, or value, or

---

[24] RESTATEMENT (SECOND) OF TORTS § 217 (1965) [hereinafter RESTATEMENT (SECOND)].

[25] 962 F. Supp. 1015 (S.D. Ohio 1997).

[26] *Id.* at 1021 (citing Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Ct. App. 1996)).

[27] *Id.* at 1024.

> (c) the possessor is deprived of the use of the chattel for a substantial time, or
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[28]

The court found that CompuServe had suffered two kinds of harm.[29] First, Cyber Promotions's messages consumed CompuServe's disk space and drained processing power.[30] The court reasoned that Cyber Promotions's use of CompuServe's resources diminished "the value of that equipment to CompuServe,"[31] thus satisfying section 218(b) of the *Restatement*. Second, the court concluded that Cyber Promotions's activities threatened CompuServe's "business reputation and goodwill."[32] Because CompuServe's subscribers paid for their Internet subscriptions in time increments, they would be likely to cancel their subscriptions if the flow of unwanted e-mail were not curtailed.[33] The court characterized this harm as harm to something in which CompuServe had a protected interest for purposes of section 218(d).[34]

Courts soon applied *CompuServe*'s reasoning in a series of bulk e-mail cases raising similar facts.[35] But *CompuServe*'s reasoning was also extended to other contexts. Plaintiffs argued that *CompuServe*'s trespass-to-chattels approach should also protect web servers from unwanted uses. In *eBay, Inc. v. Bidder's Edge, Inc.*,[36] for example, a district court held that eBay, an auction-hosting service, was entitled to enjoin Bidder's Edge, a service that gathered data concerning ongoing auctions from various sites and presented aggregate listings of those auctions, from using certain techniques to gather data from eBay's auction pages. Bidder's Edge employed an automated software tool often referred to as a "robot" to extract data from

---

28 RESTATEMENT (SECOND), *supra* note 24, § 218.

29 For further discussion of the court's handling of the harm requirement, see *infra* notes 50–54 and accompanying text.

30 *CompuServe*, 962 F. Supp. at 1022.

31 *Id.*

32 *Id.* at 1023.

33 *See id.*

34 *Id.* at 1022–23.

35 *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000) (recognizing trespass based on sending of bulk e-mail); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998) (same); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (same); *see also* Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020, 1025–26 (N.D. Cal. 1998) (granting injunction because evidence supported finding of trespass where subscriber used account with ISP to send unsolicited e-mail, which resulted in ISP being overwhelmed with misdirected replies).

36 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

eBay's site: Bidder's Edge's software would retrieve one eBay file, and would then follow all of the links in that file to retrieve other files, and so on.[37] Just as the *CompuServe* court found that the sending of e-mail constituted use of or intermeddling with CompuServe's mail servers, the *eBay* court found that Bidder's Edge's repeated requests for auction data constituted use of or intermeddling with eBay's web servers.[38] As for whether Bidder's Edge's conduct was authorized, the court observed that eBay had specifically notified Bidder's Edge of its objection to the company's use of automated queries after the parties failed to agree on licensing terms.[39]

The most difficult issue for the court was what sort of harm, if any, eBay needed to show to obtain a preliminary injunction.[40] Bidder's Edge's robots queried eBay's servers approximately 100,000 times a day, but those queries represented at most 1.53 % of the total load on eBay's servers.[41] eBay also argued that Bidder's Edge's site provided outdated pricing information, thus making Bidder's Edge's users less likely to bid on items available on eBay.[42] The court focused on the burden Bidder's Edge placed on eBay's servers, concluding that, despite the small load that Bidder's Edge's queries imposed, eBay nevertheless would be likely to demonstrate that Bidder's Edge's activities "have diminished the quality or value of eBay's computer systems."[43] The court first reasoned that even if Bidder's Edge's activities burdened eBay's servers only minimally, those activities "use[d]" a portion of eBay's property and thereby "deprived eBay of the ability to use that portion of its personal property for its own purposes."[44] eBay was entitled to block that unauthorized use. Second, if Bidder's Edge were allowed to continue querying eBay's site over eBay's objection, "it would likely encourage

---

[37] For more information on such automated software tools, see, for example, The Web Robots FAQ, *at* http://www.robotstxt.org/wc/faq.html (last visited July 27, 2004). The term "robots" is often used interchangeably with such terms as "spiders" and "crawlers," *see, e.g.*, O'Rourke, *supra* note 8, at 570, although some commentators use the term robots to connote a broader range of software tools of which spiders and crawlers are a subset, *see* Stephen T. Middlebrook & John Muller, *Thoughts on Bots: The Emerging Law of Electronic Agents*, 56 BUS. LAW. 341, 342–44 (2000). I adopt the narrower usage here.

[38] *See eBay*, 100 F. Supp. 2d at 1070 ("Conduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel.").

[39] *Id.* at 1062.

[40] *See id.* at 1064–69, 1071–72.

[41] *Id.* at 1063.

[42] *See id.* at 1062 (noting that eBay wished to permit Bidder's Edge's queries of its system only when Bidder's Edge user actually queried Bidder's Edge's servers, in part to "increase[ ] the accuracy" of data Bidder's Edge would provide regarding eBay items).

[43] *Id.* at 1071.

[44] *Id.*

other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers."[45] In granting injunctive relief, the court thus relied both on Bidder's Edge's use of a portion of eBay's servers and on the potential for harm to eBay's servers if others replicated Bidder's Edge's activities.

Although other courts have found trespass liability in similar circumstances,[46] one court questioned the *eBay* court's approach. In *Ticketmaster Corp. v. Tickets.com, Inc.*, the defendant used robots to extract data from Ticketmaster's website and aggregated that information on its own site along with event listings involving other ticket sellers.[47] The district court denied preliminary injunctive relief and later granted the defendant summary judgment on Ticketmaster's trespass-to-chattels claim. In an unpublished opinion explaining the denial of the preliminary injunction, the district court distinguished *eBay* by pointing out that Ticketmaster had made no showing that others would replicate the defendant's activities and thereby threaten to overload Ticketmaster's servers.[48] In the subsequent opinion on summary judgment, the court specifically questioned eBay's suggestion that use of a system, without more, could give rise to a claim for trespass to chattels.[49]

B. The Harm-Based Doctrinal Critique and Its Challenges

As noted above, the most difficult issue for the *CompuServe* and *eBay* courts was what harm, if any, the plaintiffs had to show to secure injunctive relief. To evaluate the courts' holdings, we can posit four approaches to the harm question that a court analyzing an electronic trespass claim could take. First, a court could hold that trespass to chattels is actionable only when the plaintiff demonstrates actual or threatened impairment of the *chattel itself*—the computer equipment.

---

[45] *Id.* The court envisioned that if other aggregators began to utilize similar types of recursive searching, "eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses." *Id.* at 1066.

[46] *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 396, 404 (2d Cir. 2004) (affirming preliminary injunction against use of automated software to extract information about new domain-name registrants from public database for solicitation purposes); *cf.* Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724, 2001 WL 1736382, at *11–*13 (N.D. Cal. Dec. 6, 2001) (declining to dismiss trespass claim based on use of automated software to copy codes from plaintiff's website).

[47] Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 WL 1887522, at *2 (C.D. Cal. Aug. 10, 2000).

[48] *Id.* at *4.

[49] Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) ("This court respectfully disagrees with other district courts' finding that mere use of a spider to enter a [publicly] available web site to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels.").

Second, a court could take a broader approach to harm and require a showing that the claimed trespass caused some physical harm to the *possessor or the possessor's property*, if not necessarily to the chattel itself. Third, a court could find a trespass actionable upon the showing of harm *proximately related* to the interference with the computer system; this approach would likely allow a court to recognize consequential economic damages, even in the absence of harm to the chattel itself or to other property. Finally, a court might conclude that, for purposes of obtaining injunctive relief, a plaintiff *need not show any harm*—that a plaintiff has an inviolable interest in her computer equipment and is entitled to enjoin any unwanted "use" of that equipment, even if such a use might not give rise to a claim for damages.

Which approaches are reflected in the *CompuServe* and *eBay* decisions? *CompuServe* did not involve actual or threatened damage to CompuServe's mail servers or other property. The *CompuServe* court did state that Cyber Promotions's messages consumed disk space and drained processing power.[50] The court characterized these effects as a "physical impact of defendants' messages on [CompuServe's] equipment,"[51] but the court did not suggest that Cyber Promotions's messages had caused or threatened to cause any impairment to CompuServe's computers or that CompuServe's equipment could not bear the burden the unwanted messages imposed.[52] Rather, the court viewed this physical impact as affecting "the *value* of that equipment to CompuServe."[53] Thus, *CompuServe* did not involve either of the two narrower harm rules requiring some physical damage to property. The court instead appeared to take the third approach, relying on projected economic harms: The unwanted e-mail would affect the value of CompuServe's servers, or would cause a loss of customer goodwill.[54]

In *eBay*, different portions of the opinion focus on different possible harms. The court at one point suggested that "use" of eBay's system alone was sufficient to entitle eBay to injunctive relief[55]—that, consistent with the fourth approach outlined above, no showing of harm was required. Elsewhere, it focused on the possibility that other

---

[50] CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).

[51] *Id.*

[52] *Accord* McGowan, *supra* note 14, at 347–48 ("There was no evidence that the plaintiff's servers crashed, that it ran out of disk space, or that its customers were actually blocked out of the system.").

[53] *CompuServe*, 962 F. Supp. at 1022 (emphasis added).

[54] *Id.* at 1022–23.

[55] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

aggregators might replicate Bidder's Edge's activities and eventually overload eBay's servers.[56] *eBay* can thus be read to have tied injunctive relief to a potential future harm to eBay's servers, a result consistent with the first approach discussed above. At the same time, it was clear that Bidder's Edge's use itself threatened no harm to eBay's system, and the court's conclusion that eBay might eventually suffer harm from the activities of other aggregators depended on numerous unstated assumptions, including that the market could support the dozens of other aggregators that would be required to impair the servers' functioning. Because these assumptions are highly questionable,[57] *eBay* seems to rely more on use than on actual harm.[58]

This question of what harm a system owner must show to obtain an injunction to block unwanted uses of her system forms the central thread in scholars' doctrinal critique of trespass cases.[59] Commentators argue that, to sustain a trespass-to-chattels claim, a plaintiff should be required to show not merely harm, but a harm to the chattel itself—that is, to the computer system that processes the unwanted communications.[60] As Professor Burk has explained, the trespass-to-chattels tort, like the tort of conversion, protects a *possessory* interest:

---

[56] *Id.* at 1066, 1071–72.

[57] *See, e.g.*, O'Rourke, *Shaping Competition*, *supra* note 13, at 1980 ("The optimal number of spiders indexing a site may be greater than one, but it is likely also to be less than the number that would cause the system to crash."). Because metasites like Bidder's Edge rely so heavily on advertising revenue, O'Rourke suggests, "[c]hances are high that the number of indexing sites that could attract enough money to remain in business is less than the number that would materially adversely affect system performance." *Id.* at 1980–81; *see also* Brief of Amici Curiae Mark A. Lemley et al. in Support of Bidder's Edge, Appellant, Supporting Reversal at 14, eBay, Inc. v. Bidder's Edge, Inc., No. 00-15995 (9th Cir. submitted June 22, 2000) ("[T]he economics of electronic commerce are such that it is doubtful that a horde of such auction aggregation services are likely to arise."); Steve Fischer, Comment, *When Animals Attack: Spiders and Internet Trespass*, 2 MINN. INTELL. PROP. REV. 139, 162 (2001) ("While . . . additional aggregators will surface . . . the market will not be able to support a multitude of spiders."). *But see* Kramer & Monahan, *supra* note 8, at 250 (comments of Jay Monahan, Senior Intellectual Property Counsel for eBay, Inc.) (arguing that even small burden on servers is problematic because "[i]f we ran everything right at capacity, it would be suicidal," and "[e]ven the slightest slow-down can directly affect trading, and that directly affects the income made by [eBay]").

[58] *Accord* McGowan, *supra* note 14, at 351 (suggesting that "the court's speculation about harm detracts significantly from the normative force of the opinion").

[59] The most extended and significant critique of courts' application of the trespass tort to network resources is Professor Dan Burk's. *See* Burk, *supra* note 14; *see also* Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. DAYTON L. REV. 179, 203–06 (2001); Hunter, *supra* note 12, at 483–88; O'Rourke, *supra* note 8, at 593–96; O'Rourke, *Shaping Competition*, *supra* note 13, at 1993–97; R. Clifton Merrell, Note, *Trespass to Chattels in the Age of the Internet*, 80 WASH. U. L.Q. 675, 687–97 (2002); Laura Quilter, Note, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 435–43 (2002).

[60] *See, e.g.*, Burk, *supra* note 14, at 34–37.

"The gravamen of both actions lies in the dispossession of the property from its owner. In conversion, the dispossession is total; in trespass to chattels, the dispossession is only partial."[61] Because the tort protects a possessory interest, Burk argues, a trespass claim should lie only when the defendant's actions affect the *physical condition* of the chattel. When a court recognizes consequential economic harms, such as a loss of subscriber goodwill, as an actionable harm for purposes of a trespass-to-chattels claim, it cuts the link between the plaintiff's possessory interest in the chattel and the harm.[62] Relatedly, scholars argue, to rest liability on mere use of a computer—with only the most speculative discussion of the possibility of harm—is to ignore the harm requirement of the tort altogether.[63]

The California Supreme Court essentially adopted this harm-based critique in *Intel Corp. v. Hamidi*.[64] The case involved Intel's efforts to enjoin its former employee, Kenneth Hamidi, from sending e-mails critical of Intel's employment policies to Intel employees through Intel's mail servers.[65] Although Hamidi sent each of his e-mails to several thousand Intel employees, he had done so only on a handful of occasions.[66] Accordingly, Intel could not plausibly claim that Hamidi's conduct had affected the functioning of its servers.[67] Intel argued both that it did not need to show harm to enjoin Hamidi's conduct,[68] and that it could in any event demonstrate two harms: first, that Intel had expended resources attempting to block and clear its systems of Hamidi's e-mails;[69] and second, that Hamidi's messages, if not blocked, would distract employees and cause a loss of productivity.[70]

The two lower courts found Intel's arguments persuasive and enjoined Hamidi's conduct.[71] The California Supreme Court reversed. Although broader language appears in isolated places in its

---

61 *Id.* at 33.

62 *See id.* at 35–37; Quilter, *supra* note 59, at 429–30, 439–41.

63 *See* Hunter, *supra* note 12, at 487; O'Rourke, *supra* note 8, at 596–97.

64 71 P.3d 296 (Cal. 2003).

65 *Id.* at 299.

66 *Id.* at 301.

67 *Id.* ("Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning."); *id.* at 303–04 (reviewing evidence on this issue).

68 *Id.* at 303.

69 *See id.* at 301 (noting Intel's "uncontradicted evidence . . . that staff time was consumed in attempts to block further messages from FACE-Intel").

70 *See id.* at 307–08 (discussing Intel's claim that messages caused loss of productivity).

71 *See* Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 247–53 (Ct. App. 2001).

opinion,[72] the *Hamidi* court adopted the first of the harm approaches outlined above, finding that Intel's trespass claims failed because Intel could not show actual or threatened damage to its computer system or impairment of its functioning.[73] The *Hamidi* court characterized its approach as a straightforward application of common-law doctrine,[74] but in fact the question is far more complicated than the *Hamidi* court suggests.

There are three main problems with the *Hamidi* court's approach. First, although the court purported to adhere to the approach reflected in bulk e-mail and robot cases, it ignored or mischaracterized key aspects of those cases. Second, the court adopted an extremely narrow and textualist reading of the *Second Restatement of Torts*, treating it as if it were a statute rather than a synthesis of an adaptive common-law doctrine. In doing so, the court downplayed the underlying interests that trespass-to-chattels doctrine protects. Third, the *Hamidi* court's harm-to-system test obscures the court's tacit judgment on the value of Hamidi's speech.

The *Hamidi* court purported to follow the approach to harm used in the earlier cases concerning unsolicited commercial e-mail and the use of robots to extract data from websites, but it was not faithful to those cases. For example, in attempting to reconcile its decision with that of the district court in *eBay*, the *Hamidi* court focused heavily on *eBay*'s suggestion that other aggregators, mimicking the activities of Bidder's Edge, could overwhelm *eBay*'s system.[75] It thus concluded that the *eBay* holding required a showing of harm or threatened harm to physical computer equipment.[76] In fact, however, the *eBay* court believed that Bidder's Edge had no right whatsoever to use eBay's system, regardless of harm: The court explicitly stated that Bidder's

---

[72] *See Hamidi*, 71 P.3d at 307 n.6 (raising possibility that trespass-to-chattels claim could be sustained upon showing of harm to possessor or possessor's other property, but stating that Intel raised no claim of such harm).

[73] *See id.* at 300 (stating that trespass to chattels does not cover "an electronic communication that neither damages the recipient computer system nor impairs its functioning," because tort requires "interfere[nce] with the possessor's use or possession of, or any other legally protected interest in, *the personal property itself*" (emphasis added)); *id.* at 303 (stating that dispositive issue is whether Hamidi's actions "caused or threatened to cause damage to Intel's computer system, or injury to its rights in *that personal property*" (emphasis added)).

[74] *See id.* at 302 (discussing "[c]urrent" California tort law); *id.* at 306 (stating that portions of *eBay* decision did not reflect "correct statement of California or general American law"); *id.* at 308 (characterizing claim that no showing of harm should be required to sustain injunctive relief as proposing "[e]xtension" of California tort law).

[75] *Id.* at 306.

[76] *Id.*

Edge's "use" of eBay's system "deprived eBay of the ability to use that portion of its personal property for its own purposes."[77]

Similarly, the *Hamidi* court characterized *CompuServe* as involving potential harm to CompuServe's mail servers. *CompuServe*, of course, recognized certain economic damages attributable to Cyber Promotions's alleged trespass, including the Internet service providers's (ISP's) loss of business reputation and customer goodwill.[78] While acknowledging that *CompuServe* involved economic harm, the *Hamidi* court strained to link that harm to some physical harm to CompuServe's property. The *Hamidi* court noted that CompuServe's "system" was "inundated with unsolicited commercial messages."[79] The court thus implied that the unsolicited e-mail affected the functioning of CompuServe's computer system—that is, CompuServe's *mail servers.* The court then observed that CompuServe's asserted injuries were more closely connected to CompuServe's personal property than were the asserted injuries in *Hamidi*, since it was "*the functioning of CompuServe's electronic mail service*" that prompted CompuServe's customers' complaints.[80] By subtly shifting its focus from CompuServe's *servers* to CompuServe's *service*, the *Hamidi* court obscured the fact that the harm CompuServe claimed was not actual or threatened impairment of its computer system, but rather the loss of customer goodwill. Because *CompuServe*'s customers' complaints were truly about the cost of sifting through e-mail,[81] and there was no evidence that CompuServe's servers could not bear the burden that Cyber Promotions's e-mails imposed,[82] the link between the economic damages and the chattel in *CompuServe* is functionally equivalent to the link between Intel's claimed economic damages and the chattel in *Hamidi.* In both cases, quite apart from any physical effect on the computer system, the unwanted communications allegedly had an economic effect on the system owners' businesses. Indeed, although the *Hamidi* court went to great lengths to distinguish the bulk e-mail cases by establishing that it was the "content" of Hamidi's messages that prompted Intel's objection, providers' objec-

---

[77] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

[78] *See supra* notes 50–54 and accompanying text.

[79] *Hamidi*, 71 P.3d at 307 (noting that "CompuServe's customers were annoyed because the *system* was inundated with unsolicited commercial messages, making its use for personal communication more difficult and costly" (emphasis added)).

[80] *Id.*

[81] CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997).

[82] *See supra* note 52 and accompanying text.

tions in the bulk e-mail cases were likewise based on the *content* of the e-mail rather than on some physical effect to the computer system.[83]

The fact that *Hamidi* mischaracterized *eBay* and *CompuServe* does not itself suggest that the court's approach was wrong. *eBay* involved a federal district court applying California law, a subject on which the California Supreme Court has the last word; and, of course, the *Hamidi* court was free to reject the interpretation of Ohio law reflected in the *CompuServe* case. But the *Hamidi* court also took an extremely narrow view of the trespass-to-chattels tort. As noted earlier, according to section 218(b) of the *Second Restatement of Torts*, one is liable for trespass to chattels if one dispossesses another of a chattel or causes some kind of harm, including impairing the chattel "as to its condition, quality, or value."[84] The court held that only actual or threatened impairment of the functioning of the system could affect its "condition, quality or value."[85] One could argue, however, that a server's "value" is tied to the contributions the equipment makes to the owner's revenue model. When the foreseeable consequence of interference with the computer system is a cost imposed on the owner, perhaps the concept of "value" of the chattel should capture the cost.[86]

Section 218(d) of the *Restatement* also links liability to harm "to some person or thing in which the possessor has a legally protected interest."[87] Although the *Hamidi* court did not specifically cite that clause, its conclusion that a trespass claim will lie only upon a showing of impairment to the computer system necessarily rested on the pre-

---

[83] *See* Burk, *supra* note 14, at 37 (noting that "impairment" in *CompuServe* amounted to "no more than the receipt of annoying content").

[84] *See supra* note 28 and accompanying text.

[85] *Hamidi*, 71 P.3d at 304 (rejecting Intel's contention that its interest in physical condition, quality, or value of its computers was harmed and concluding that "the decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning").

[86] Professor Burk, like the *Hamidi* court, adopts a narrow interpretation of "value." In particular, he suggests that when unwanted contacts cause no damage to the equipment, the value of the equipment is not impaired because the owner could sell it for just as much after the unwanted contacts as before. *See* Burk, *supra* note 14, at 35 (linking concept of "value" under § 218(b) of *Restatement* to market price). His conception of injury, however, is incomplete. If one purpose of applying trespass to chattels in this context is to preserve incentives for productive uses of computer resources, *see infra* notes 106–07 and accompanying text, the market-price approach alone is clearly insufficient, for even the most extreme forms of hacking might not alter the market price of computer equipment. A market-price approach to "value" could be appropriate, so long as economic injuries are actionable elsewhere within the trespass-to-chattels tort. As discussed in the text, however, the *Hamidi* court narrowly interpreted the other prongs of section 218 as well and thus seemed to reject any relief for economic injury.

[87] *See supra* note 28 and accompanying text.

mise that consequential economic damages such as loss of productivity or loss of goodwill do not qualify as something in which the system owner has a "legally protected interest."[88] It is worth noting, however, that the *Hamidi* court's approach to economic damages creates some perverse incentives. Because only actual harm (or the threat of harm) to the computer system triggers liability, liability depends not on the character of the defendant's activities, but on the (in)ability of the plaintiff's computer system to absorb the effects of those activities. The greater the processing power of a company's computer system, the less likely it is that unwanted contacts will impair its functioning. In other words, if the trespass-to-chattels tort protects a resource owner's possessory interest in her equipment, that possessory interest is surely an odd one because the interest of a computer owner with a large system receives less protection than the interest of a computer owner with a small system.[89]

Even if the *Hamidi* court's interpretation of the language of the *Restatement* is correct, the broader point is that one cannot parse the language of the *Restatement* as if it were a statute. The *Restatement* merely synthesizes an adaptive common law doctrine, and more important than the *Restatement*'s specific language is the underlying interest the *Restatement* seeks to protect. Indeed, just as it is possible to read the *Restatement* to foreclose liability for purely economic harms arising from interference with a chattel, it is possible to read the *Restatement* to permit injunctive relief for a trespass-to-chattels claim even when a plaintiff shows no harm at all. The commentary accompanying section 218 on harm states that one cannot sue on a trespass-to-chattels theory for nominal damages, offering the following explanation:

> The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. . . . Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.[90]

---

[88] *Cf. Hamidi*, 71 P.3d at 307 (noting assertion in *CompuServe* that loss of business reputation and customer goodwill constituted harm to "the ISP's legally protected interests in its personal property"); *id.* at 308 (stating that Intel could not assert property interest in its employees' time).

[89] As David McGowan points out, this result is especially odd if capacity is costly because the system owner who sinks the most money into her network has the least ability to control it. McGowan, *supra* note 14, at 369.

[90] RESTATEMENT (SECOND), *supra* note 24, § 218 cmt. e.

The *Hamidi* court read this passage to foreclose liability for trespass to chattels in the absence of a showing of some harm[91]—as suggesting that a possessor has no legally protected interest in the inviolability of her chattel. The passage, however, supports precisely the opposite conclusion. First, the comment does not in fact suggest that a possessor lacks a legally protected interest in the inviolability of a chattel; indeed, it acknowledges that interest and deems it "similar" to the interest of a possessor of land. Rather, the comment says that, unlike with trespass to land, one is not entitled to *nominal damages* to protect that interest in inviolability. The unavailability of a nominal-damages remedy for past, harmless intermeddling with a chattel says nothing about whether a possessor is entitled to injunctive relief to prevent future activities—and injunctive relief was the only relief that the *Hamidi* court considered.[92] More fundamentally, the comment presupposes that a possessor can protect the interest in inviolability of a chattel through exercising a privilege of self-help.[93] All of the electronic trespass cases involved self-help. The particular self-help efforts the plaintiffs chose, however, were only temporarily effective or were altogether unavailing because the defendants found a way to evade them, and because escalating them would have affected other legitimate customers. For example, Intel attempted to block Hamidi's e-mail, but Hamidi evaded its efforts by sending his e-mails from different computers;[94] likewise, Cyber Promotions circumvented CompuServe's blocking mechanisms by falsifying the point-of-origin information in its e-mail headers and concealing the IP addresses of its computers.[95] Such cat-and-mouse games—with plaintiffs attempting to erect technical barriers to block certain activity and defendants finding ways to evade them—are common to all of the major Internet trespass-to-chattels cases.[96]

---

[91] *Hamidi*, 71 P.3d at 302–03.

[92] Intel initially sought damages, but later waived the claim. *Id.* at 301.

[93] For similar arguments, see Epstein, *supra* note 14, at 78–81 (suggesting that privilege to use reasonable force to protect chattel ordinarily preserves possessor's "inviolate" interest in chattel, but that "pressure on these rules has mounted with the rise of the internet"); McGowan, *supra* note 14, at 356 (arguing that Internet trespass cases "do not alter the real-world results that would occur if, as the *Restatement* contemplates, self-help worked").

[94] *Hamidi*, 71 P.3d at 301.

[95] CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019 (S.D. Ohio 1997).

[96] *See, e.g.*, Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 896 (N.D. Iowa 2001) (noting defendant's awareness that "his e-mailers were the subject of anti-spam efforts by ISPs such as AOL"); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1062 (N.D. Cal. 2000) (noting that eBay blocked 169 IP addresses it believed Bidder's Edge was using to query eBay's systems, but that Bidder's Edge used proxy

Indeed, it is worth noting that the *Hamidi* court's apparent conclusion that a system owner does *not* have an inviolable interest in her computer system leads to some odd results. The *Hamidi* court's approach would in theory permit a defendant to evade *technical* restrictions on access to a computer system so long as the defendant caused no harm to the system.[97] Suppose that, rather than sending employees e-mail, Hamidi had hacked into Intel's web servers and briefly replaced the main web page with that of his anti-Intel organization, FACE-Intel—a practice known as "graffiti hacking." While such action would have both interfered with Intel's web servers and deprived Intel of the use of some portion of its web server, under the *Hamidi* court's reasoning, such graffiti hacking would not be tortious because it threatened no physical harm to or impairment of the functioning of Intel's web servers.

A defender of the *Hamidi* court's approach might argue that evading a technical restriction to replace content on a server is more troublesome than merely sending e-mail to servers configured to receive e-mail. That conclusion, however, depends on an assumption that the law should enforce access restrictions coded into software, but should not enforce limitations a system owner conveys by other means, such as actual notice (a point I challenge in Part III).[98] The defender might also suggest that other sources of law, including computer crime statutes, sufficiently regulate activities like hacking.

---

servers to evade blocks); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998) (noting defendants' efforts to "evade AOL's filtering mechanisms").

The back-and-forth between Ticketmaster and Tickets.com appears to have gone through numerous rounds. *See* Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (noting Ticketmaster's significant expenditure of "time and effort" to "frustrate" Tickets.com's spider); Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 WL 1887522, at *2 (C.D. Cal. Aug. 10, 2000) (discussing Ticketmaster's thwarted efforts to redirect incoming Tickets.com traffic from its interior pages to its main pages); Appellants' Opening Brief at 10, Ticketmaster Corp. v. Tickets.com, Inc., 2 Fed. Appx. 741 (9th Cir. 2001) (No. 00-56574) ("Tickets.com designed its spiders to deceive Ticketmaster's computers into believing that the electronic signals generated by Tickets.com's spiders were generated by a Netscape browser utilizing a Windows 95 operating system; when they do not."). In addition, according to Ticketmaster, Tickets.com used other methods to elude Ticketmaster's blocking technology, including accessing Ticketmaster's servers through various ISPs. *Id.* It would have been impossible for Ticketmaster to exclude the spiders without also excluding Internet users utilizing the same ISPs.

[97] For a case that seems to reach precisely that conclusion, see Pearl Invs., LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326, 349–50, 353–54 (D. Me. 2003) (dismissing claim that unauthorized connection of server to plaintiff's virtual private network, thus creating "tunnel" into network, constituted trespass to chattels).

[98] *Cf.* McGowan, *supra* note 14, at 371 (posing question as "whether the law should require password protection as a condition of recognizing the right to exclude, or whether it should [also] recognize that right when 'open' websites object to particular uses").

Perhaps so, but the point for now is that *Hamidi*'s harm-to-system approach implies that even breach of these sorts of technical restrictions should not be actionable as trespass.

Finally, even if the harm-to-system approach is correct, its application in the *Hamidi* decision serves as a rather transparent cover for a quite different rationale: that Hamidi's message was sufficiently valuable that its distribution should be permitted. Assume, for example, that Hamidi had distributed pornographic e-mails to Intel's employees rather than e-mails concerning Intel's review and promotion policies. Under the *Hamidi* court's approach, Intel could not enjoin such communications. Any harm that such messages cause would be functionally equivalent to the harm of Hamidi's messages; and, as in *Hamidi*, Intel's objection would have been based on the content of the e-mail. In other words, the harm-to-system approach prevents Intel from excluding not only e-mails that are critical of its policies but also other communications that it might find objectionable based on content.

It nevertheless seems doubtful that the court would have denied Intel an injunction if Hamidi had attempted to distribute pornography. That point highlights the distinction between the harm-to-system approach the *Hamidi* court nominally adopted and the "nuisance" approach some commentators have favored.[99] Under a nuisance approach, a court would weigh the social value of the tortfeasor's use against the harm to the system owner. A nuisance rationale explains why a court might assign liability for the transmission of pornographic e-mails but not for e-mail such as Hamidi's—a pornographic e-mail has limited social value, while an e-mail criticizing employment practices may have significant social value. But the consequences of shifting from a harm-to-system approach to a true nuisance approach are significant. Denying Intel the legal means to block Hamidi's e-mail at first seems to be a victory for free speech, but, importantly, it limits Intel's speech by preventing the company from tailoring its space to particular uses.[100] In addition, at least in a case involving the transmission of e-mail, a nuisance approach necessarily places a court in the position of making content-based judgments about the social value of different uses of a system. To the extent that the *Hamidi* court's decision reflects the court's conclusion that Hamidi's use *was* socially valuable, the decision is all the more troubling for its silence on that point.

---

[99] *See supra* note 14.

[100] *See* McGowan, *supra* note 14, at 360–66 (arguing that right to exclude "plays a vital role in constituting the social function of different spaces" and allows for "[m]anagerial discretion over the expressive environment of the workplace").

None of this, of course, establishes that the *Hamidi* court's conclusion was incorrect. Rather, the point is that, from a doctrinal perspective, the matter is far more complicated than has been portrayed by the *Hamidi* court and those scholars who oppose application of trespass to chattels in the Internet context. A court faced with an electronic trespass claim seeking injunctive relief must choose a particular approach to the question of harm. The *Hamidi* court, in essentially embracing commentators' critiques of the bulk e-mail and robot cases, adopted an approach that requires a plaintiff alleging a trespass to chattels to demonstrate that a defendant's actions threaten to damage or impair the functioning of her computer system itself. As will be discussed later, carrying that approach to its logical conclusion would be a risky step.

C. *Normative Critiques*

In order to truly understand the potential significance of the *Hamidi* opinion for the shape of the Internet and for the development of access control technologies, we must examine why, among the different rules for harm, commentators have advocated harm-to-system or nuisance approaches. The remainder of Part I considers the normative ideas that underlie scholars' objection to utilizing trespass-to-chattels doctrine in the Internet context. More broadly, setting aside the doctrinal requirements for particular cyberproperty claims, it asks how the law *should* protect network resources.

By way of introduction, it is useful to begin our examination of potential regulatory approaches to unwanted use of network systems by introducing the classic dichotomy between "property" and "liability" rules.[101] Under a property rule, the law recognizes an entitlement holder's right to enjoin any unwanted uses of a protected asset, whether or not the use will cause harm.[102] Because the entitlement

[101] *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972). For discussion and refinements of the Calabresi and Melamed framework, see, for example, Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027 (1995); Abraham Bell & Gideon Parchomovsky, *Pliability Rules*, 101 MICH. L. REV. 1 (2002); Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 HARV. L. REV. 713 (1996); James E. Krier & Stewart J. Schwab, *Property Rules and Liability Rules: The Cathedral in Another Light*, 70 N.Y.U. L. REV. 440 (1995); Saul Levmore, *Unifying Remedies: Property Rules, Liability Rules, and Startling Rules*, 106 YALE L.J. 2149 (1997); Carol M. Rose, *The Shadow of* The Cathedral, 106 YALE L.J. 2175 (1997).

[102] Calabresi & Melamed, *supra* note 101, at 1092 ("An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller.").

holder can block any unwanted use, she can set the terms of access to a resource, requiring potential users of the system to negotiate for access.[103] Protecting network computing resources under a property rule would allow the resource owner to weigh the costs and benefits of particular uses and determine which uses to allow. In contrast, under a liability-rule approach, the would-be user has the right to utilize the entitlement holder's asset, subject to terms determined by a third party (typically, a court or legislature).[104] A liability-rule approach to network resources would allow access against the property owner's wishes but might require payment of damages for certain harmful activities.[105] Applying either type of rule with respect to network resources could in theory yield the same level of access. For example, even if a website owner can set the terms of access (a property-rule approach), she may choose to allow all access that does not impair her system, on the theory that such access will be beneficial. This approach would result in the same degree of openness as would a liability rule that allowed access but required a user to pay for any harm to the system. Thus, in choosing between property-rule protection and liability-rule protection for resources, the issue is not only *what level of access* to network resources is appropriate, but also *who should decide* what level of access is appropriate—the resource owner or a third party (such as a court or legislature).

The *Hamidi* court rejected a property-rule approach: Under the court's trespass-to-chattels framework, companies like Intel would lack the ability to enjoin unwanted e-mail or to set the terms of access to their mail servers. Most scholars addressing the cyberproperty controversy concur, arguing that property-rule protection for network resources is wholly inappropriate; and this line of argument guided the court's decision in *Hamidi*. The remainder of this section explores scholars' arguments and shows that those arguments do not make a conclusive case against a property-rule approach. I do not seek to make an affirmative case for a property-rule approach here. By exposing certain gaps and weaknesses in the prevailing normative critiques of cyberproperty claims, however, I hope to set the stage for a fuller analysis of the issues in Parts II and III.

---

103 *Id.*

104 *See id.* ("Whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule.").

105 The classic example of a liability rule is a nuisance: A factory owner may pollute a nearby resident's air, but must pay damages. *See id.* at 1116.

1. *The Competing Interests in Cyberproperty Claims*

Before evaluating the normative arguments against granting a network resource owner a right to exclude unwanted uses, we should identify the competing interests at stake in cyberproperty disputes. These competing interests are well illustrated by the trespass-to-chattels cases considered in Sections A and B.

First, the law must provide sufficient protection of a network resource owner's investments—both in physical equipment and in the development of a business model—to generate appropriate incentives for productive activities.[106] The *CompuServe* and *eBay* decisions reflect courts' sensitivity to this problem. In *CompuServe*, the defendants had essentially shifted to CompuServe (and its subscribers) some of the costs of transmitting bulk e-mail, and CompuServe's lawsuit reflected an effort to shift those costs back to the defendants. If the law required ISPs to bear the full cost of the transmission of unsolicited commercial e-mail, they would be less likely to provide such services.[107] Similarly, companies such as eBay are less likely to develop online business models if they cannot protect against a competitor's free riding.

Second, the public has an interest in open access to information and open avenues for speech. If a company such as eBay can control access to its servers, it can also control access to the information those servers hold. eBay may have objected to Bidder's Edge's extraction and aggregation of its data in part because it feared that Bidder's Edge (though not a direct competitor) would draw customers away from its site.[108] But search engines and comparative shopping utilities

---

[106] *See* Madison, *supra* note 12, at 436 (noting that various doctrines invoked to protect access to systems share policy goal that "investments in efforts to produce and distribute intangible information should be legally protected as a way to preserve incentives to make those investments"); Jane K. Winn, *Crafting a License to Know from a Privilege to Access*, 79 WASH. L. REV. 285, 285 (2004) (noting that application of trespass-to-chattels doctrine to Internet raises competing interests in protecting "incentives to invest in the kind of commercial facilities that now largely constitute the Internet" and "the public interest in knowledge gleaned from information posted on the Internet").

[107] The recently enacted federal statute regulating unsolicited commercial e-mail practices is premised in part on this fact. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 2(a)(6), 117 Stat. 2699, 2699–700 (to be codified at 15 U.S.C. § 7701(a)(2)(6)) (noting "significant monetary costs" imposed on providers of Internet access services).

[108] *See* Elkin-Koren, *supra* note 59, at 182 (arguing that eBay objected to Bidder's Edge's activities because "eBay sought to preserve its dominance in the online auction industry" and that, if Bidder's Edge prevailed, eBay's users would "no longer be captured and restricted to a single site"). As I argue below, however, the claim that eBay's motive for denying access to Bidder's Edge was anticompetitive is difficult to square with eBay's willingness to license other aggregators, as long as they would agree to post only current price data. *See infra* note 195 and accompanying text.

work in precisely the same way as Bidder's Edge, by using software programs to recursively query sites and aggregating and organizing the resulting data for users. Granting a website owner the power to block a competitor's robots also grants the site owner the ability to block a search engine's robots, thus raising the possibility that property-rule protection for systems will curtail one of the most publicly beneficial features of the Internet.[109] Likewise, as evidenced by the *Hamidi* case, power to control access to mail servers can translate easily into a power to curtail objectionable speech. The California Supreme Court's sympathy with Hamidi's defense appeared to stem from its concern that Intel was seeking to suppress dissent about its policies—that the case implicated free-speech interests, albeit at the level of policy rather than at the level of the Constitution.[110]

Third, even setting aside questions about how information available on the Internet is ultimately used and about the extent to which the Internet provides open avenues for speech, society has an interest in the scale of the network itself. The Internet reflects what economists term "network effects" or positive "network externalities": Access to the network becomes more valuable as it becomes more widespread.[111] Consider an analogy to a telephone system. With only a few subscribers, such a system has very little value. As subscribership grows, however, the value of the system to each subscriber increases.[112] Similarly, each user's access to the Internet becomes more valuable as use of the Internet becomes more widespread. When a service provider or website owner blocks unwanted access, the service provider essentially closes a portion of the network and thereby limits the network's scale.[113]

Finally, assuming the law does permit system owners to enforce some restrictions on the use of network resources, users have an interest in fair notice of the conditions of access. Most Internet resources appear to users to be available without any restrictions on access, in the sense that there is no *technical* impediment (such as a

---

109 *See infra* notes 165–66 and accompanying text.

110 *See* Intel Corp. v. Hamidi, 71 P.3d 296, 307–08 (Cal. 2003) ("Intel's position represents a further extension of the trespass to chattels tort, fictionally recharacterizing the allegedly injurious effect of a communication's *contents* on recipients as an impairment to the device which transmitted the message.").

111 For discussion of the theory of network effects, including its distinct variants and their manifestation in several different fields of law, see generally Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998).

112 Burk, *supra* note 14, at 50–51 (explaining theory of network effects through example of telephone system); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1281 (1998) (same).

113 *See infra* notes 170–76 and accompanying text.

password restriction) to users sending e-mail to most mail servers or retrieving files from most web servers. Because the lack of any technical impediment to access can signal the resource owner's consent to the use in question, the law must require a resource owner to provide adequate notice of deviations from an open access condition. In *CompuServe* and *eBay*, of course, the defendants had actual notice of the system owners' objection to the unwanted use.[114] Both cases also raised, but did not resolve, questions about the adequacy of alternative forms of notice—in CompuServe's case, a policy available on its network prohibiting unsolicited commercial e-mail, and in eBay's case, a user agreement that prohibited automated queries of its system.[115]

2. *"Overpropertization" Critiques and Their Limitations*

The question then becomes: What sort of legal protection for network resources best balances the competing interests identified above? To date, most scholars have rejected property-rule protection in the Internet context. The next two subsections evaluate the arguments against property-rule protection.

As noted earlier, both property rules and liability rules in theory can yield an optimal amount of access. Which sort of rule is preferable often depends on how likely it is that the rules will in fact yield a socially optimal amount of access. According to the conventional view of how the legal system should protect entitlements, property rules are favored when transaction costs—including the costs of identifying and bargaining with the parties to a dispute, and the costs of obtaining information on how the parties value a particular entitlement—are low.[116] When transaction costs are low, bargaining will lead to an efficient distribution of entitlements, and there is no need (from an efficiency perspective) for legal intervention to influence that distribution. When transaction costs are high, and the parties cannot easily identify and bargain with one another, bargaining will not occur, and the result will be an inefficient distribution of entitlements. In this context, liability rules may be preferable.[117]

Although it is fair to describe this account as the conventional one,[118] significant law-and-economics scholarship is devoted to chal-

---

114 *See supra* notes 27, 39 and accompanying text.

115 *See infra* notes 235–38 and accompanying text.

116 Calabresi & Melamed, *supra* note 101, at 1127.

117 *Id.*

118 *See* Ayres & Talley, *supra* note 101, at 1037 (describing transaction costs account as "folklore" among law-and-economics academics); Kaplow & Shavell, *supra* note 101, at 718 (challenging "conventional wisdom" on the virtues of property versus liability rules);

lenging it.[119] As a result, it is not surprising that some arguments against courts' recognition of cyberproperty claims come from within this framework, while others come from outside the framework. I turn first to general arguments against property-rule protection for network resources, and then to arguments that depend more directly on the costs of bargaining and problems of valuation. What all of the arguments have in common is a concern that recognition of cyberproperty claims will lead to "overpropertization" of the Internet—that system owners' ability to assert a strong property right to exclude unwanted uses will curtail productive uses of the Internet.

a. Cyberproperty Claims as Enclosure of Intellectual Property

As noted, one of the difficulties raised by cyberproperty claims is that a right to control access to the physical equipment of a network translates into far broader powers—for example, the ability to block speech or to control access to and uses of information.[120] It is intellectual property law—specifically copyright law—that ordinarily establishes the extent to which one can control uses of informational goods. The control that copyright law provides, moreover, is incomplete.[121] Accordingly, scholars fear that recognizing a system owner's right to block unwanted uses of network resources will shift informational goods from a copyright regime of incomplete protection to a property regime of complete protection.[122] As I will show, however, there are two problems with this argument. First, the argument assumes that the incentives that intellectual property law provides for the development of informational goods are sufficient for the development of online business models. Second, taken to its logical conclusion, the anti-enclosure position points to a fully mandatory access approach, under which sites could not use password protection or any other sort of technical self-help to block unwanted uses. Scholars do not seem to embrace that conclusion.[123] Yet, in accepting that system owners may use some technical measures to "close" access to a site, scholars do not explain why technical limitations on access are permissible, but other limitations are not.

Krier & Schwab, *supra* note 101, at 447–55 (criticizing as "simplistic conventional wisdom" notion that liability rules are always appropriate when transaction costs are high).

[119] *See generally* Ayres & Talley, *supra* note 101; Kaplow & Shavell, *supra* note 101; Krier & Schwab, *supra* note 101.

[120] *See supra* note 12 and accompanying text; *infra* notes 165–66 and accompanying text.

[121] *See infra* notes 126–31 and accompanying text.

[122] *See infra* notes 139–47 and accompanying text.

[123] *See infra* notes 155–57 and accompanying text.

A significant and growing body of literature on developments in copyright law suggests that the public domain is shrinking, as informational goods traditionally treated as part of the "commons" achieve legal protection as private property.[124] As Professor James Boyle has put it, we are in the midst of a "second enclosure movement," a phrase intended to evoke comparison with the conversion of common areas into private property in England from the fifteenth through the nineteenth centuries.[125] Copyright law traditionally has not granted creators of informational goods so-called "strong" property rights—that is, clear and undivided entitlements.[126] Because uses of informational and other intangible goods are non-rival, one of the main justifications for recognizing strong property rights—the threat that resources available to all will be overused—does not apply to intellectual property.[127] Accordingly, the law recognizes a copyright holder's exclusive rights to control uses of her work only for a limited period of time,[128] and subjects those rights to particular limitations, such as the public's right to make fair use of the work and a range of compulsory licenses.[129] Moreover, because copyright law only protects original works of authorship—a standard that requires some modicum of creativity—not all works achieve copyright protection.[130] In particular, facts do not warrant copyright protection, nor do insufficiently original compilations of facts.[131]

---

124 *See, e.g.*, Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 354–55 (1999); James Boyle, *Cruel, Mean or Lavish? Economic Analysis, Price Discrimination and Digital Intellectual Property*, 53 VAND. L. REV. 2007, 2010 (2000); James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33, 37–40 (2003) [hereinafter Boyle, *Second Enclosure Movement*]. For a discussion of the origins of the overpropertization critique with respect to copyright law, see Benkler, *supra*, at 354 n.2.

125 *See* Boyle, *Second Enclosure Movement*, *supra* note 124, at 33–36 & nn.2, 9 (describing first enclosure movement).

126 *See, e.g.*, Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 136 (1999) (observing that federal copyright system recognizes variety of weak entitlements, including "muddy" and divided entitlements).

127 *See* Boyle, *Second Enclosure Movement*, *supra* note 124, at 41 (noting that "informational or innovational commons" does not involve same threat of overuse as physical commons); Carol M. Rose, *Romans, Roads, and Romantic Creators: Traditions of Public Property in the Information Age*, 66 LAW & CONTEMP. PROBS. 89, 90 (2003) (observing that "Tragedy of the Commons" argument does not apply with respect to intangible property because "there is no physical resource to be ruined by overuse").

128 *See* 17 U.S.C. § 302 (2000).

129 *See id.* §§ 107–112, 115.

130 *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991) ("The *sine qua non* of copyright is originality. To qualify for copyright protection a work must be original to the author.").

131 *Id.* at 344, 348. For opposing perspectives on the implications of *Feist* for protection of databases, compare Jane C. Ginsburg, *Copyright, Common Law, and* Sui Generis *Pro-*

Critics of recent trends in copyright law suggest that copyright's limited protection for informational goods strikes a delicate balance between providing incentives for the creation of such goods and preserving public access to them.[132] That balance, the critics argue, is threatened by a range of legal developments permitting purveyors of informational goods to achieve greater protection than copyright law has traditionally recognized—that is, to secure strong property rights. To take one example, providers of information in digital form can use "rights management systems"—technical mechanisms that allow a provider to dictate what uses are and are not permitted, and at what price—to control uses of a digital work, effectively deploying a technical fence around the information, regardless of whether copyright law or related doctrines would protect it.[133] The permissions the information provider sets effectively become a self-enforcing substitute for the provisions of copyright law.[134] Relatedly, if copyright law does protect the work, and technical measures control access to it, the Digital Millennium Copyright Act prohibits their circumvention,[135] even if the user seeks to make fair use of the work.[136] Commentators

tection of Databases in the United States and Abroad, 66 U. CIN. L. REV. 151, 176 (1997), favoring additional protection of databases, with J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 137–38 (1997), criticizing proposals for *sui generis* protection of databases.

132 *See* Boyle, *Second Enclosure Movement*, *supra* note 124, at 42–44 (explaining incentive argument for intellectual property protection and innovation benefits from public access to information); Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1098 (2003) ("[T]he use of intellectual property law is always a balancing act between allowing the greatest number of people to enjoy works at low cost, without lowering the cost so much that the works will never be created in the first instance."); *see also* Benkler, *supra* note 124, at 401–08 (opposing expansion of copyright and related rights on ground that such expansion is unlikely to increase information production in aggregate).

133 *Compare, e.g.*, Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 48 (2001) (arguing that rights management systems "will allow copyright owners to appropriate far more protection than copyright law now provides"), *and* Lemley, *supra* note 112, at 1291–92 (commenting that "[t]here is no reason to expect that technological protection systems designed for the benefit of copyright owners will preserve" uses that copyright law always permitted), *with* Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 561 (1998) (identifying public benefits of rights management systems). For a discussion of how rights management systems work, see *id.* at 565–67 & nn.31–40.

134 *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 135–36 (1999).

135 *See* 17 U.S.C. § 1201(a)(1)(A) (2000).

136 *See* Benkler, *supra* note 124, at 415 (noting that anticircumvention prohibition "operates irrespective of whether the access gained . . . infringes a property right in the work"); Burk, *supra* note 132, at 1102 ("Anticircumvention laws used as an adjunct to technological controls confer upon content owners a degree of control never attainable under a regime of traditional copyright."); Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 839–40 (2001) (noting that violation of DMCA does not depend on whether access led to

treat these and a range of other developments, from copyright term extensions[137] to proposals aimed at protecting uncopyrightable databases,[138] as part of this "unprecedented" enclosure trend.

The normative concerns scholars raise with respect to cyberproperty claims fit within the context of this larger debate. Applying trespass-to-chattels doctrine in a dispute over access to a web server or similar system may allow the system owner to restrict access to and use of material made available on that system, regardless of whether copyright law protects the material.[139] For example, as mentioned above, copyright protection does not extend to facts or insufficiently original compilations of factual information, such as the white pages of a telephone directory.[140] If similar information were held on a website, and a court recognized a system owner's right to block unwanted uses through trespass to chattels or another claim, the court would effectively grant to system owners a right to control information broader than that granted by copyright law. Likewise, the Computer Fraud and Abuse Act, the federal analogue to state trespass claims, prohibits unauthorized access to "information,"[141] regardless of whether intellectual property law protects the material in question.[142] If a system owner can block any use of material on a website based on the objection that the system owner did not authorize access to its computer system, the CFAA provides an alternative cause of action when copyright protection is unavailable.[143]

---

infringement or fair use); *see also* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 543–46 (1999) (describing legitimate reasons for circumvention that DMCA does not recognize).

137 *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 106 (2001) ("The distinctive feature of modern American copyright law is its almost limitless bloating—its expansion both in scope and in duration.").

138 *See* Benkler, *supra* note 124, at 440–46 (outlining and criticizing proposed Collections of Information Antipiracy Act (CIAA), which would prohibit extraction or use of data from databases and collections of information that are currently uncopyrightable).

139 *Cf.* Burk, *supra* note 14, at 39–40, 43–44 (alleging that Internet-based trespass-to-chattels claims are an attempt to gain protection copyright law will not provide).

140 Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 363 (1991).

141 18 U.S.C. § 1030(a)(2)(C) (2000).

142 *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 324 (2004) (arguing that "by allowing website owners to protect information that is not protectable under copyright law, the CFAA unconstitutionally overrides the delicate balance of rights between authors and the public").

143 Similarly, although the DMCA's anticircumvention provision covers only works protected by copyright law, it raises some of these same difficulties. To the extent that a system owner uses a technical protection measure to control access to a work with copyrightable and noncopyrightable elements, the DMCA appears to prohibit circumvention to gain access to the noncopyrightable portions. Moreover, as noted, the law validates an

Similarly, if a court applies contract principles to enforce a system owner's "terms of use," and allows the agreement to govern even when its terms are inconsistent with copyright law, the terms of use displace more limited copyright protections.[144] In such a case, the owner's right may sound in contract rather than property, but if courts do not carefully scrutinize whether the user had notice of and manifested assent to the contract terms, the owner's contract rights take on the characteristics of property rights.[145]

Scholars thus argue that if intellectual property law does not protect particular material, then other doctrines and methods should not; otherwise the balance that intellectual property law strikes between providing incentives to create and preserving public access will be undermined.[146] In other words, by granting protection above and beyond intellectual property law, a cyberproperty rule grants benefits to producers that go further than necessary to incentivize production of the underlying work. It effectively becomes a transfer of wealth from consumers to producers.

To counter this concern that tort and contract law are "enclosing" otherwise unprotected digital material, critics argue for rejecting

---

owner's use of technical protection measures regardless of whether a user seeks to make fair use of the work. *See supra* note 136 and accompanying text.

144 *See, e.g.*, Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1095–96 (1998) (noting that "legal protection against unauthorized copying and distribution is incomplete, and is so by design," and discussing courts' treatment, as a matter of contract law, of mass-market standard forms, which share some features with terms of use); Margaret Jane Radin, *Regulation by Contract, Regulation by Machine*, 160 J. INSTITUTIONAL & THEORETICAL ECON. 1, 6 (2004) (noting that provision of terms of use can "supersede[ ] copyright law by extending control of the property owner to information that the copyright law delimits as non-property").

145 *See* Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CAL. L. REV. 111, 119–21 (1999) (arguing that because proposed uniform law governing transactions in information "abandon[s] the focus on offer and acceptance, . . . contracts [under that law] are really more akin to property rights"); *cf.* Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 496 n.118 (1998) (noting convergence of contract reasoning and property reasoning); Lemley, *supra* note 112, at 1259 n.7 (discussing property/contract convergence).

146 *See, e.g.*, Burk, *supra* note 14, at 39–40 (arguing that trespass to chattels reflects "a novel, hybrid form of a property right" that shares "the same concerns as previous attempts to subject Internet activity to a strict regime of exclusory rights"); *id.* at 43 (criticizing trespass to chattels on ground that it reflects "an attempt to address the same issues that copyright has allowed to pass unsanctioned in web linking"); Elkin-Koren, *supra* note 59, at 208–09 (arguing that because copyright law "was designed to regulate use and information, and . . . includes some checks and balances informed by the unique character of informational works and their social significance[, t]he displacement of copyright law by other common-law doctrines for establishing a right to control access to information is worrisome"); O'Rourke, *Restrictions on Access*, *supra* note 13, at 296 (arguing that courts evaluating cyberproperty claims "have been less receptive than they should be to considerations of copyright policy").

cyberproperty claims and thereby preserving application of copyright law to define the scope of the system owner's rights.[147] Scholars urge courts to use one of several tools to achieve this preservation of copyright law. Some scholars argue that copyright law should be understood to preempt application of state trespass[148] and contract principles.[149] Others claim that there are constitutional limits on enclosure of the public domain, either in the First Amendment[150] or in the Copyright Clause itself.[151] On this view, the perceived excessive enclosure of the public domain that application of cyberproperty claims would entail is unconstitutional.

Scholars typically acknowledge, however, that courts would have to adjust the current contours of copyright preemption[152] and adopt a more expansive view of the role of the Constitution in policing the boundary between intellectual property rights and the public domain[153] to preserve the application of copyright principles where scholars believe they should apply. The argument, quite simply, is normative rather than doctrinal, and measuring it against the competing interests outlined in Part I.C.1 above reveals its weaknesses.

Cyberproperty critics attach paramount importance to the interest in preserving open access to information. As for the role of

147 *See, e.g.*, O'Rourke, *Restrictions on Access*, *supra* note 13, at 296 ("Courts should not adopt a perspective that cedes all questions of terms of access and use to laws other than copyright.").

148 *See* O'Rourke, *supra* note 8, at 590 ("If 'accessing' is synonymous with 'copying,' then the Copyright Act is the exclusive rule of decision under its preemption section. There is simply no room for a state law 'trespass to a website' cause of action." (citation omitted)); O'Rourke, *Restrictions on Access*, *supra* note 13, at 306–07 (suggesting that implied preemption analysis might find trespass tort preempted by copyright law); *see also* Burk, *supra* note 14, at 40 (labeling trespass cause of action "[c]opyright's [c]ousin").

149 *See* Elkin-Koren, *supra* note 59, at 200 ("A license that restricts the use of (otherwise unprotected) information could be preempted under copyright law."); O'Rourke, *Restrictions on Access*, *supra* note 13, at 300–04 (proposing and working through preemption analysis for contract terms).

150 *See* Benkler, *supra* note 124, at 393 (arguing that "all property rights in information conflict with the 'make no law' injunction of the First Amendment").

151 *See* Galbraith, *supra* note 142, at 358 (arguing that "it is highly unlikely that Congress even has the power to create private property rights in factual information").

152 *See, e.g.*, Elkin-Koren, *supra* note 59, at 200 n.80 (noting holding in *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), that contractual restrictions on use of information are not preempted by copyright law); Lemley, *supra* note 145, at 139–44 (discussing fact that Copyright Act's preemption provision, 17 U.S.C. § 301 (2000), "does not seem to preempt most contractual provisions," and that, despite potential for implied conflicts preemption based on conflict between copyright policy and state contract enforcement, law remains inconsistent and underdeveloped in this area).

153 *See, e.g.*, Yochai Benkler, *Through the Looking Glass: Alice and the Constitutional Foundations of the Public Domain*, 66 LAW & CONTEMP. PROBS. 173, 198 (2003) (describing "decidedly contested" view "of the constitutional framework that constrains Congress from regulating information and cultural production too greatly").

the law in providing incentives for investments in the development of an online business, however, the anti-enclosure position simply seems to presume that the incentives copyright law supplies are sufficient—that any incentives above those copyright law provides simply transfer wealth from consumers to producers. When we focus on the interest in open access to the exclusion of the interest in providing incentives, however, it becomes difficult to say why the law should even grant a system owner a right to block uses that cause physical harm to a system. In other words, if all websites should remain part of a "commons," it is unclear why a private party should have a right of action even if her computer system is harmed.[154] The fact that most scholars do accept that a system owner can block uses that will cause harm to her system suggests that scholars are in fact more sensitive to the incentive issues than their predominant focus on the preservation of open access would at first suggest. But once we recognize that some protection of a system is necessary to guard investments in an online business model, it is unclear why the law should recognize physical harm and not economic harm. The anti-enclosure position simply provides no basis for accepting one harm rule and rejecting another.

Second, even if intellectual property law does provide the relevant incentive structure, relying on intellectual property law to displace application of cyberproperty claims faces another problem. In particular, taken to its logical conclusion, the anti-enclosure position would suggest that systems connected to the Internet cannot use password protection to control access to their websites. I know of no scholar who advocates this sort of fully mandatory open-access approach. Scholars do criticize the DMCA on the ground that, in prohibiting circumvention of technical measures to control access to a copyrighted work, it puts the force of law behind a copyright holder's terms of access; some scholars go so far as to argue that would-be users should have the right to circumvent technical measures to gain access to a work to make a fair use.[155] Scholars do not, however, suggest that a website must remain open to all would-be users. Rather, they seem to view the decision to disallow some access—by "closing" sections of the site—as a permissible and legitimate choice.[156] The

---

154 *See* McGowan, *supra* note 14, at 368.

155 *See, e.g.*, Cohen, *supra* note 144, at 1141–42 (suggesting that recognizing right to "hack" digital rights management systems "simply reaffirms the balance between authors and users, and between information ownership and the public domain").

156 *See, e.g.*, Burk, *supra* note 14, at 54 (noting that "any consent to system usage that might be implied from connection to the Internet surely does not include 'hacker' intrusion"); *see also id.* at 38 (focusing critique of trespass-to-chattels claims on cases in which connection to Internet gives rise to inference of "invitation" to engage in certain conduct, such as transmission of files over e-mail system).

question is why the decision to limit access through password protection is permissible, but the decision to impose other kinds of limitations is not.[157] The anti-enclosure story simply cannot answer that question.

Relatedly, an approach that relied wholly on the contours of intellectual property law to establish when access to a system is permissible would prohibit a website owner from using other sorts of self-help measures to control the circumstances under which others gain access to the site. For example, eBay's and Ticketmaster's efforts to block requests for data based on the IP address of the computer seeking the data, or efforts to redirect requests for information to a main page rather than an interior page,[158] would be illegitimate because, like a legal right to exclude unwanted uses, such self-help measures allow enclosure of information that copyright law does not protect. Again, I know of no scholar who suggests that these sorts of self-help measures are impermissible. Here, the anti-enclosure argument reaches another logical impasse: Scholars remain wedded to the notion of open access but ignore its implications.

In sum, although arguments challenging enclosure trends make many compelling points with respect to intellectual property law, those arguments ultimately cannot explain why courts should reject cyberproperty claims. Scholars seem to assume that intellectual property law provides adequate incentives for the development and delivery of web content. Even if they are correct, their argument points to a position that no one ultimately takes—that system owners cannot use even the most basic technical protections.

b. Bargaining and Valuation Problems Under a Property-Rule Approach

As the discussion above suggests, arguments relying on the balance intellectual property law strikes between control and access do not conclusively establish the case for rejecting cyberproperty claims. I turn here to other normative arguments scholars offer to explain why granting system owners the right to exclude unwanted uses will result in overpropertization. In particular, scholars offer three main reasons why recognizing cyberproperty claims will curtail productive uses of the Internet. First, they claim, Internet transactions are sufficiently complex that granting resource owners a right to exclude

[157] I return to one plausible answer below—that a system owner who does not password-protect but who otherwise seeks to control access is free-riding on the network by taking advantage of its openness but refusing to contribute to its scale. *See infra* notes 170–76 and accompanying text.

[158] *See supra* note 96 and accompanying text.

unwanted uses of their systems will prevent optimal uses.[159] Second, if resource owners are left to balance the competing interests at stake, they will be likely to undervalue the benefits of open access.[160] Finally, scholars fear that if system owners are granted a right to exclude, they will exercise that right in an anticompetitive manner.[161] I highlight problems with each of these arguments.

First, scholars seem to assume that protecting network resources through a property-rule approach is the equivalent of setting a default rule of closed access, regardless of a system's technical configuration. That assumption, of course, factors heavily into scholars' assessment of when users must negotiate for access and thus of whether productive uses of the Internet are likely to occur. A default rule of closed access, however, is not an inevitable feature of a property-rule approach.[162] Removing that assumption undermines much of the force of the scholarly critiques. Second, like the intellectual property critique, some of the arguments logically lead to a fully mandatory access rule that few commentators actually would advocate. Finally, although it is difficult to gauge the risk of anticompetitive conduct, concerns about such conduct are difficult to reconcile with existing cyberproperty cases. In addition, it is possible to respond to such concerns without entirely rejecting property rule forms of protection.

In arguing that the law should not grant network resources owners a right to exclude unwanted uses of their systems, scholars claim that recognizing cyberproperty rights will force potential users to bargain for access in such a wide range of circumstances that productive uses simply will not occur. Some critics go so far as to suggest that validation of access controls, particularly through the application of trespass doctrine, will lead to the creation of an "anticommons"—a form of property in which rights are "so finely divided" that it is impossible to make optimal use of a resource.[163] The argument draws upon Professor Michael Heller's work on post-Soviet Russia, which attributed suboptimal uses of certain property to the excessive division in the "bundle" of rights typically associated with ownership of private property, resulting in parties' inability to bargain to efficient uses of resources.[164] Some scholars suggest that recognition of access

159 *See infra* notes 165–69 and accompanying text.

160 *See infra* notes 170–76 and accompanying text.

161 *See infra* notes 177–79 and accompanying text.

162 *See infra* pp. 2207-08.

163 Burk, *supra* note 14, at 49; *accord* Hunter, *supra* note 12, at 511.

164 *See, e.g.*, Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998) [hereinafter Heller, *The Tragedy of the Anticommons*]. For articles applying the concept of the anticommons and exploring its effects, see generally Hanoch Dagan & Michael A. Heller, *The Liberal Com-*

controls will create a digital anticommons: If system owners have a right to exclude unwanted uses, then users must negotiate licenses with the owners of each system they wish to access on the Internet. As Professor Burk has put it, "One can imagine the anti-commons nightmare that could ensue on the Internet in web linking, indexing, and other routine functions if every owner of equipment attached to the network were granted a cause of action for the trespass of unwanted electrons on her equipment."[165] Similarly, Professor Dan Hunter has suggested that, if the law recognizes a right in system owners to exclude unwanted uses, search engines "will be severely constrained" and aggregation products will disappear.[166] He even asks, only somewhat rhetorically, whether application of a trespass cause of action to unsolicited e-mail might imply

> that one must read the "Terms of Acceptable Email Usage" of every email system one emails in the course of an ordinary day[.] If the University of Pennsylvania had a policy that sending a joke by email would be an unauthorized use of its system, then under the logic of [trespass-to-chattels case law], you would commit "trespass" if you emailed me a *Calvin and Hobbes* cartoon.[167]

Even those who do not specifically invoke the anticommons problem suggest that recognizing a right to enjoin unwanted contacts will curtail productive uses of the Internet. Professor Lawrence Lessig argues that under the approach of the *eBay* court, if "individual sites begin to impose their own rules of exclusion," the costs of using the Internet will climb because "machines must negotiate before entering any individual site."[168] Likewise, a brief filed by dozens of intellectual property and cyberlaw professors in the *Hamidi* case suggested that, under a trespass approach, "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel."[169]

Apart from concerns about the range of circumstances in which bargaining must occur for productive activities to go forward, scholars seem to raise a second concern: that system owners will tend to undervalue the system-wide benefits of granting access. This concern emerges from scholars' claims that the Internet itself is a "commons"

---

mons, 110 YALE L.J. 549 (2001); Michael A. Heller, *The Boundaries of Private Property*, 108 YALE L.J. 1163 (1999); Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCI. 698 (1998).

165 Burk, *supra* note 14, at 49.

166 Hunter, *supra* note 12, at 508.

167 *Id.* at 508–09.

168 LESSIG, *supra* note 137, at 171.

169 Intel Corp. v. Hamidi, 71 P.3d 296, 310 (Cal. 2003).

that is increasingly being enclosed.[170] Commentators point to the fact that the Internet developed and flourished with open access to the communications protocols needed to transmit information and nondiscriminatory access to the Internet backbone.[171] Recall the observation that the Internet is a prime example of "network effects"—that a connection to the Internet becomes more valuable as use of the Internet becomes more widespread.[172] Those who connect computer systems to the Internet, whether they offer subscribers capabilities to send and receive mail or host information, benefit from the scale of the network,[173] and as individual sites "begin to impose their own rules of exclusion, the value of the network as a network declines."[174] It is unfair, scholars suggest, for system owners to reap the benefits of a large-scale network while refusing to bear costs associated with it.[175] Moreover, because system owners cannot fully internalize the benefits that derive from the scale of the network, they will be likely to exclude uses that might contribute to the scale.[176]

Third, scholars suggest that system owners have incentives to block access to their systems for anticompetitive reasons. This argument has been most thoroughly developed by Professor Maureen O'Rourke. She observes that, although many websites are unlikely to object to uses such as indexing by a search engine's robots, the best-known sites "may prefer that users travel directly to them rather than first going to a search engine from which they may choose to go to a competitive site."[177] In essence, firms wish to preserve market power, and dispersal of product and pricing information by a search engine may erode brand power and bring markets closer to perfect competition.[178] Although O'Rourke concedes that the choice between recog-

---

170 *See* Hunter, *supra* note 12, at 503–04.

171 *See, e.g., id.*; Lemley, *supra* note 12, at 534–36.

172 *See supra* notes 111–12 and accompanying text.

173 *See* LESSIG, *supra* note 137, at 171 (noting that sites such as eBay benefit greatly from open network); Burk, *supra* note 14, at 51 (describing positive network externalities involved in companies' use of Internet).

174 LESSIG, *supra* note 137, at 171.

175 *See* Burk, *supra* note 14, at 48 (noting that companies such as Intel "derive[ ] benefit from the public nature of network"); *id.* at 51 ("[P]ropertization in a networked environment encourages the holder of the exclusive right to attempt to free-ride upon the external benefits of the network, while at-will avoiding contribution of such benefits to others."); Hunter, *supra* note 12, at 502 (arguing that "'cyberspace enclosure movement'" began when "online actors, who had cheerfully reaped the benefits of the online commons, decided to stake out their own little claims in cyberspace").

176 Burk, *supra* note 14, at 48 (arguing that "there are public benefits to be had in a cyberspace network that are not captured, and indeed may be destroyed by overpropertization").

177 O'Rourke, *Shaping Competition*, *supra* note 13, at 1975.

178 *Id.* at 1977–78.

nizing strong or weak property rights in network resources presents a "close" question, she argues that strong exclusionary rights are inappropriate in the early stages of development of electronic commerce.[179]

How persuasive are these arguments against a property-rule approach to protecting network resources? Several of the claims seem overbroad. Consider, first, commentators' claim that the Internet itself is a "commons" that is increasingly being enclosed. It is true that the functioning of the Internet relies on access to common resources donated to transferring and relaying information and to protocols that enable all parties connected to the Internet to communicate with other systems.[180] But to make the case that recognizing a network resource owner's right to exclude unwanted access will enclose the Internet commons, one must argue that network endpoints, such as mail servers and web servers, have historically been part of the commons as well. That is a far more difficult case to make.[181] To the extent that we *do* treat network endpoints as part of the commons, moreover, these resources may be subject to the same forces that justify property rights in other contexts. For example, mail servers face a fairly typical "tragedy of the commons" problem: Because those who transmit e-mail do not bear the cost of the use, they are likely to overuse the resource. The solution to a "tragedy of the commons" problem, in most instances, is to propertize it.[182]

---

[179] *Id.* at 2005.

[180] *See* Hunter, *supra* note 12, at 503–04.

[181] In a recent article, for example, Professor Dan Hunter argues that application of trespass to chattels in the Internet context results in enclosure of the Internet commons. But Hunter's concept of what forms the Internet "commons" is unclear. Hunter first focuses on the communications protocols that allow computers to communicate with others on the network and the resources donated to relaying and transferring information. *Id.* at 503–04. To the extent that he treats network endpoints such as mail servers as part of the commons, he focuses on the role of mail servers in relaying e-mail messages on behalf of other systems. *Id.* at 503. That mail servers sometimes performed these functions on behalf of other systems, however, does not mean that mail servers granted unfettered access for any and all uses. When discussing the problem of the "enclosure" of the Internet commons, Hunter is careful to focus on the communications protocols and network resources donated to relaying and transferring information—he asks that we "[c]onsider the 'property' at issue *not as individual websites or mail systems*, but rather the commons property of the network resources." *Id.* at 511 (emphasis added). Despite having never made the case that "individual websites or mail systems" were open to any and all uses, however, Hunter then suggests that "[w]e used to enjoy a general and untrammeled 'right' of access to websites, email systems, fileservers, and so forth" and that a right to exclude unwanted uses from a web server or a mail server will therefore constitute "enclosure" of the commons. *Id.*

[182] *See, e.g.*, Rose, *supra* note 127, at 90 (presenting "tragedy of the commons" argument as one rationale for exclusive property rights).

Web servers may not be subject to the same tragedy of the commons. The argument that web servers should remain part of the commons, however, still encounters the same difficulties as the general concern about enclosure of information on web servers.[183] The argument begs the question of whether intellectual property law provides the only appropriate incentive structure for encouraging investment in productive activities online. In addition, the Internet-as-commons position cannot support any rule short of mandatory open access: If web servers and mail servers are a "commons," they should be open to any and all uses. It quickly becomes impossible for system owners to justify the use of any technical measures such as passwords to protect their sites.

Another claim that seems exaggerated is that granting a system owner a right to block unwanted access will result in the development of a digital "anticommons." In identifying the anticommons as a form of property, Professor Heller described situations in which rights with respect to a single piece of property are divided among many parties,[184] and in which a particular parcel of land is fragmented into unusable portions (as in the case of successive devises).[185] Recognition of access controls on the Internet simply cannot be compared to the first situation: The Internet is not a single piece of property, the efficient use of which is prevented by dispersal of the typical rights of ownership. An Internet in which access controls are validated might be closer to the fragmented parcel of land. Fragmentation of real property, however, presents problems that do not exist in the Internet context. Where consolidation of the property cannot be achieved by operation of law, parties must negotiate to re-form the parcels into a usable piece of land; one party can hold out and prevent the efficient use of the resource.[186] But no similar holdout problem exists on the Internet. The fact that one site blocks a search engine's recursive queries from retrieving information for indexing purposes does not mean that recursive queries cannot retrieve information from sites that do permit such activities. It is obvious that enforcing access controls might make a search engine less useful than it otherwise might be, but to state that concern in the form of an appeal to the "anticommons" is

---

183 *See supra* notes 153–58 and accompanying text.

184 Heller, *The Tragedy of the Anticommons*, *supra* note 164, at 680 ("Privatization broke up the socialist bundle of corporate governance rights among a heterogeneous set of managers, workers, and local governments. These new owners may now hold excessive rights of exclusion, such that each prevents the others from restructuring corporate assets.").

185 *Id.* at 685–87 (discussing "anticommons" problems associated with congressional allotment of Native American communal lands).

186 *See* Burk, *supra* note 14, at 49 (describing holdout problem).

to take as a given that the entire Internet must be open, when that is precisely the question in dispute.

Even if we trim away these broader claims, we are still left with a core argument that cyberproperty rights will reduce the availability of information on the Internet—that bargaining must but will not occur in a wide range of circumstances. Recall the arguments of Professors Burk, Hunter, and Lessig, as well as those of the dozens of intellectual property and cyberlaw professors in *Hamidi*: that routine functions such as linking and indexing would be blocked by recognition of trespass to chattels;[187] that the logical extension of applying trespass to chattels to mail servers is that one must consult the terms of use for every system to which one transmits e-mail;[188] that "machines must negotiate before entering any individual site";[189] that "each of hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel."[190] In short, commentators suggest that recognizing access controls will convert a range of seemingly mundane activities into tortious conduct.

But is this necessarily so? It is worth observing that over the several years during which scholars have made dire predictions about the harmful consequences of recognizing cyberproperty claims, the predictions have remained just that. Although numerous courts have recognized cyberproperty claims, no scholar to my knowledge has yet offered evidence that electronic commerce has been harmed in any way.[191] As a matter of logic, moreover, the view that recognizing cyberproperty claims will bar routine uses is counterintuitive; the fact that system owners connect their computer systems to the Internet indicates that they desire those systems to be used in some way. Under these circumstances, it is fair to presume that system owners who connect their systems to the Internet implicitly consent to certain uses of those systems. In other words, saying that the law should grant the owner of a network resource the right to block unwanted uses

---

187 *See supra* note 165 and accompanying text.

188 *See supra* note 167 and accompanying text.

189 *See supra* note 168 and accompanying text.

190 *See supra* note 169 and accompanying text.

191 A comparison of the amicus brief filed by a group of law professors in the *eBay* case and that filed in the *Hamidi* case is instructive. Despite the two-year gap in filing dates, during which several courts recognized cyberproperty claims, the arguments are virtually identical. *Compare* Brief of Amici Curiae Mark A. Lemley et al. in Support of Bidder's Edge, Appellant, Supporting Reversal at 8–11, eBay, Inc. v. Bidder's Edge, Inc., No. 00-15995 (9th Cir. submitted June 22, 2000), *with* Brief of Amici Curiae Professors of Intellectual Property and Computer Law, Supporting Reversal at 10–12, Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (No. S103781).

does not mean that users must proceed from a default presumption of closed access.

Scholars' concerns that users must proceed from a default presumption of closed access must therefore be based on a prior premise—that even if a network resource owner consents to *some* uses of her system, a user is poorly positioned to identify the contours of that consent and must therefore either bargain for access or forgo the desired use. If, for example, a search engine developer must consult the terms of use of any site it wishes to index before using automated software to extract the contents of the site, it is unlikely that the project will go forward. Put another way, to recognize a right to exclude unwanted uses of network resources is to grant a right to control property with boundaries that are unclear, through an invitation with murky terms. On this view, recognizing a cyberproperty right raises both efficiency concerns and fairness concerns because users will not know the conditions of access.

These efficiency and fairness concerns, however, do not necessarily point toward a rejection of cyberproperty claims. In fact, the concerns point in two possible directions: toward rejecting property-rule protection, or toward recognizing a right to exclude only if system owners provide meaningful notice of the terms of access or employ technical measures that block access. Indeed, concerns about the clarity of notice may explain why even those scholars who generally oppose recognition of cyberproperty claims stop short of arguing that system owners cannot use password restrictions to segregate and control access to content.[192] Password protection provides a very clear signal to a potential user concerning restrictions on use of the system. Other kinds of limitations on permissible uses of a system—such as limitations included in a policy posted at some location on a network—do not signal the terms of access as clearly.

These responses to the broad efficiency and fairness concerns do not resolve the final concern that prompts scholars to resist strong property protection for network resources: that system owners will disallow access for anticompetitive reasons.[193] At the outset, it is worth noting that most of the cases in which courts have recognized cyberproperty claims do not appear to involve anticompetitive concerns. The case most often cited as demonstrating an anticompetitive use of a cyberproperty claim is the *eBay* case.[194] In fact though, eBay

---

[192] *See supra* text accompanying note 157.

[193] *See supra* notes 177–79 and accompanying text.

[194] *See* Elkin-Koren, *supra* note 59, at 182 (arguing that "eBay sought to preserve its dominance in the online auction industry"); O'Rourke, *supra* note 8, at 607 (exploring Bidder's Edge's arguments that eBay sought to control information so as to maintain its

both licensed other aggregators to index its site and agreed to allow Bidder's Edge to do so; eBay simply insisted that Bidder's Edge's queries occur in real time.[195] It is difficult to reconcile eBay's willingness to allow dispersal of its pricing information with concerns about anticompetitive conduct.[196]

Even if certain system owners *do* have incentives to use a right to exclude in anticompetitive ways, it does not necessarily follow that property-rule protection for network resources is always inappropriate. Current law generally responds to anticompetitive conduct through antitrust law—from within the existing framework of property rights, not by divesting firms of property rights. Moreover, in advocating rejection of strong property rights, most scholars do not embrace a rule that would respond directly to anticompetitive concerns by requiring system owners simply to bear certain costs of competition. Rather, scholars embrace far broader rules—rules that, for example, would require system owners to bear *any* economic harm, not merely those costs most directly associated with competition.[197]

As this discussion suggests, the case against property-rule protection for network resources is far less compelling than it appears at first glance. The issues, at least with respect to trespass to chattels, cannot easily be resolved at the doctrinal level. Normatively, arguments based on "overpropertization" of informational goods or of the Internet fail to explain why the law nonetheless should protect against uses that cause physical harm to a computer system; why, if the law does protect against such physical harm, it should not also protect

---

monopoly in online auction market); O'Rourke, *Shaping Competition*, *supra* note 13, at 1975–76 (noting eBay's "vociferous" opposition to auction indexing sites).

[195] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1062 (N.D. Cal. 2000).

[196] In this regard, O'Rourke's arguments are quite balanced. She acknowledges that a rule giving a system owner the ability to control access to product and pricing information does not raise concerns "if sites have no practical incentive" to exercise that control. O'Rourke, *supra* note 8, at 601. She argues, however, that there are "[s]cenarios . . . in which a monopolist may use its power to control the flow of information in an anticompetitive and inefficient way." *Id.* at 609.

[197] For example, under the nuisance approach advocated by Professor Burk and others, the law would require open access so long as the public benefits of access outweigh the costs to the system owner. *See supra* note 14. This response is far broader than required to address concerns about anticompetitive conduct. Professor O'Rourke's approach is perhaps the most closely tailored to anticompetitive conduct. She advocates a misappropriation model, under which courts could consider, among other things, both the cost to the objecting site of gathering the information that would be taken through the unwanted use, and whether the free-riding at issue in the unwanted use would threaten the system owner's incentives to engage in an online business. *See* O'Rourke, *Shaping Competition*, *supra* note 13, at 2001–02. An approach like O'Rourke's could allow courts to police anticompetitive behavior without destroying the incentives of companies to develop online business models and protect the security of their systems.

against economic harms; why it is permissible to use password protection to "close" a website; or why, if it is permissible to use password protection to limit access to a system, other sorts of limits are impermissible. Moreover, the normative account is clearly based on the premise that a property rule will lead to closed access, while a liability rule will lead to open access. In the next Part, I offer a broader normative framework for considering cyberproperty claims that calls this premise into question.

II
REGULATORY APPROACHES IN LAW AND CODE

Part I illustrated the doctrinal and normative complexities of network resource owners' claims to control unwanted access to their systems. I argued that such claims cannot easily be resolved at the doctrinal level. Examining the question within the standard framework of property-rule and liability-rule protection for entitlements illustrated that the case against a property-rule approach is not as compelling as scholars have assumed it to be. This Part attempts to offer a more nuanced normative framework for exploring how the law should protect network resources. I first argue that the property rule/liability rule dichotomy is fundamentally incomplete in this context. A variety of possible approaches to protecting network resources combine both property-rule and liability-rule features, in that access is allowed unless and until a system owner takes certain steps to trigger a right to block unwanted uses. These approaches are conceptually equivalent; they differ only in what kind of steps the system owners must take to trigger the right to exclude. The challenge for those who would reject certain approaches is to explain why, despite the conceptual similarity, some approaches are preferable to others.

Second, I argue that in favoring certain kinds of legal rules, scholars have not fully considered the relationship between law and technical measures in producing regulatory outcomes. As scholars have suggested in other contexts, technical measures can supplement or supplant law in producing regulatory outcomes.[198] The issue of control over network resources illustrates that point: A technical control over use of network resources can be combined with legal protection to give a system owner a significant degree of control; and even in the absence of any legal protection, a system owner can still exercise some control through technical measures. Although these issues have been explored in other contexts,[199] the cyberproperty controversy

[198] *See infra* notes 391–96 and accompanying text.
[199] *See infra* notes 391–407 and accompanying text.

illustrates another important facet of the relationship between law and technical measures. If technical measures and law both affect regulatory outcomes, and if system owners are free to choose the technical measures that protect their systems, then we must be concerned about the effect that the choice of particular legal rules will have on a system owner's selection of technical measures. In other words, it is not merely the case that law and technical measures supplant or supplement one another as regulatory forces. Law may actually produce a greater reliance on protective technology.

Section A introduces four possible legal approaches for protecting network resources. Section B further refines this analysis by providing concrete examples of each and illustrating that the approaches overlap to some extent. Sections C and D explain the relationship between law and technical measures in producing particular regulatory outcomes and reconceptualize the debate over cyberproperty claims in light of that relationship.

A. Four Legal Approaches to Protecting Network Resources

To expand the normative framework for analyzing claims to control access to network resources, it is useful to describe four possible approaches the law could take to protecting such resources. Each of the first three approaches contemplates recognizing a system owner's right to enjoin unwanted uses and thus to control the terms of access; in that sense, each involves property-rule protection. The approaches differ only in what triggers the right to injunctive relief to enforce the access conditions the system owner establishes. Under the fourth approach (a commons approach), the law will not back the system owner's terms of access with injunctive relief, thus reflecting rejection of property-rule protection.

Closed Access Default. First, the law might simply treat all access that has not been bargained for as illegitimate—that is, presume a default rule of closed access. Under this approach, the user would bear the full burden of identifying the contours of permissible use and would bear the full risk that her activities might be inconsistent with restrictions the network resource owner places on access. This approach is not unlike how trespass doctrine applies to land when the would-be trespasser has no basis to presume that a landowner consents to particular activities. To be liable for trespass, a person need not even know that he has entered onto someone else's land, as long as he intends to be where he is.[200] The presumption in law is that all

[200] *See* RESTATEMENT (SECOND), *supra* note 24, § 163 cmt. b. The comment reads in full:

uninvited entry onto property is unlawful. If the law applied an analogous presumption in the Internet context, then users would have to bargain for access to any system.

Notice-Based Approach. Under an alternative approach, the law would presume a default rule of open access, but would nevertheless allow a network resource owner to enjoin unwanted uses of her system once he or she identified limitations on the contours of permissible use. Rather than placing the full burden and risk of identifying appropriate uses on the user, the law would require system owners to "signal" limitations on use of the system, through measures reasonably calculated to give users notice of those limitations. I defer the question of what measures would meet the standard.[201] The point for now is that under this approach, the system owner would have to take some steps to secure a right to enjoin unwanted uses, but would not need to resort to technical measures actually designed to block access before receiving legal protection.

Code-Based Approach. Under a third approach, the law would require a network resource owner to do more than merely give clear notice of what uses of her system are permissible. To achieve legal protection, the system owner would need to use technical mechanisms designed to limit access—essentially to "fence" or otherwise segregate information. Technical mechanisms—such as password protection or re-routing all requests for data to a main page—designed to control access might also serve the purpose of signaling the contours of permissible access; but to trigger a system owner's legal right to enjoin unwanted uses, those mechanisms would actually have to control access to some degree. Just as a system owner can use a range of measures of varying strength to notify users of the contours of permissible access, so too can a system owner use a range of technical mechanisms of varying strength to block access. I defer the question of how effective a technical measure must be to trigger a right to enjoin unwanted uses. The point for now is that under this approach the law would back mechanisms that are actually effective in controlling some

---

> If the actor intends to be upon the particular piece of land, it is not necessary that he intend to invade the other's interest in the exclusive possession of his land. The intention which is required to make the actor liable under the rule stated in this Section is an intention to enter upon the particular piece of land in question, irrespective of whether the actor knows or should know that he is not entitled to enter.

Id.

201 *See infra* notes 326–43 and accompanying text.

access, but not mechanisms that merely signal limitations on permissible uses of a system.[202]

Commons Approach. Finally, the law might not afford the system owner any power to enjoin unwanted uses; the law would instead permit users to access any and all network resources, even over the objection of the resource owner. Even evading a technical limitation on access would not give rise to liability. I refer to this approach as a "commons" approach, to signify the absence of strong property rights in network resources.

B. Variance Within and Blurring Between Legal Approaches

In identifying the four possible approaches under which the law could protect network resources, I do not intend to suggest that there is a clear line of demarcation separating each approach from the others. Rather, the categories reflect ranges along a spectrum, and there is a considerable variance within each category and blurring between categories.

For example, it should be obvious that if the law backs relatively "weak" signaling mechanisms—mechanisms unlikely to provide notice of the range of permissible uses of a system—the result will be similar to that produced by a default rule of closed access. Consider a

---

[202] A recent article by Professor Orin Kerr addressing the scope of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C.A. § 1030 (West 2000 & Supp. 2004), distinguishes between "contract-based" and "code-based" restrictions on use of a computer system. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1599–1600, 1644–46 (2003). I use the term "code-based" restriction in a broader way than Kerr, to encompass any technical measure designed to restrict access, regardless of its strength. Kerr does not specify how strong a technical restriction must be for its circumvention to trigger a violation of the CFAA's prohibitions on unauthorized access, but the examples he offers involve fairly strong technical measures (such as password protection and encryption). *See id.* at 1664, 1666. Kerr's "contract-based" restrictions also seem to represent a subset of my category of "notice-based" restrictions. As I discuss below, disputes over unwanted access often involve "terms of use" that present difficult questions of notice and assent, *see infra* notes 239–46, 264–305, 316–24 and accompanying text, and it may be inappropriate to treat such terms as part of a binding "contract." In addition, as Kerr recognizes, it would be inappropriate to treat a system owner's mere objection to an unwanted use as a contractual restriction. *See* Kerr, *supra*, at 1639–40 (discussing Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004)). That begs the question, however, whether a system owner is limited to contractual or code-based restrictions on use of a system—or whether the owner has a "property" interest in her system that can be controlled simply by revoking any implied consent to use the system. Kerr confines his discussion to the CFAA, and thus does not address the broader normative questions raised by cyberproperty claims generally. With respect to the unauthorized access provisions of the CFAA, however, I ultimately arrive at the same conclusion as Kerr—that those provisions should be interpreted to reach only the circumvention of strong code-based restrictions. *See infra* Part III.C.1.

system owner who simply places a policy statement at some location on her network where a user is unlikely to encounter that statement, and requires no manifestation of assent to its terms. If a court nevertheless permits such a statement to govern the terms of access, then the system owner can, at very little cost, achieve nearly the same level of protection as would be achieved through a default presumption of closed access. If, on the other hand, the law requires actual and specific notice to a would-be user that particular uses are unwelcome, then a system owner must take certain significant, affirmative steps—such as policing the system to detect unwanted uses and notifying would-be users of impermissible conduct—before benefiting from legal protection.

In between these two points are other degrees of signaling that a system owner could use to convey legally enforceable limitations. As I will discuss below, one of the most difficult questions in this context is how the law should treat "terms of use" by which system owners typically purport to restrict access to their systems.[203] With no inquiry into whether terms of use are reasonably calculated to provide notice to users of the contours of permissible access, terms of use are analogous to the sort of policy statements discussed above, and a system owner receives a great deal of legal protection with little effort. If, on the other hand, such terms of use are permitted to govern only when a defendant clearly had notice of and assented to those terms, then a system owner must do more to earn legal protection.

In a similar vein, consider the use of the "robot exclusion standard" to deter automated queries of computer systems. The robot exclusion standard is a protocol by which system owners can signal from what files, if any, robots are permitted to extract data. The server owner creates a simple text file, labeled "robots.txt," that includes directives on what portions of the server may and may not be recursively queried.[204] For example, the robots.txt file may instruct *all* robots not to query *any* of the files available on the server, may instruct *all* robots not to query *certain* directories or files, or may instruct *specific* robots not to query *all* or *some* directories or files.[205]

---

[203] *See infra* notes 239–46, 264–305, 316–24 and accompanying text.

[204] *See* Web Server Administrator's Guide to the Robots Exclusion Protocol, *at* http://www.robotstxt.org/wc/exclusion-admin.html (last visited Aug. 20, 2004). The robot exclusion standard requires that the robots.txt file be placed in the top level of a server's document space—as, for example, http://www.domainname.com/robots.txt. *Id.* Because the robots.txt files appear in consistent locations, a compliant robot knows which files on a server to query.

[205] Server owners take a wide range of approaches. For example, eBay currently allows all robots access to all but three of its directories, although it includes a comment (unreadable by robots) in its robots.txt file purporting to disallow them. *See* http://www.ebay.com/

Software developers who adhere to the robot exclusion standard simply program their agents to access and follow the instructions in the robots.txt file at every site they visit. Adherence to the robot exclusion standard is "voluntary" in the sense that the web server will not actually deny access to a robot that ignores the information in the robots.txt file.[206] The standard nevertheless serves as a means to provide technical but very specific notice about permissible uses of a system. Assuming the law gives effect to limitations on access if the system owner uses measures that clearly convey them to would-be users, the question is whether limitations conveyed through terms of use or the robot exclusion standard qualify as such measures.

We can also identify some blurring between notice-based and code-based approaches. For example, a system owner might set forth terms of use and require users to click an "I Agree" button before proceeding—perhaps even requiring the user to scroll through all of the terms before clicking "I Agree." In this context, the system owner may merely be attempting to signal limitations on use of the system, but the requirement to click "I Agree" also acts as a very weak technical control on access.

Just as there are a range of signaling mechanisms that vary in how likely they are to provide users with notice of the permissible uses of a system, there are a range of code-based mechanisms that vary in how likely they are to actually block access to a system. Consider the example of a system owner who wishes to control access to her site based on the address of the page from which the user was referred to the site. The *Ticketmaster* case provides a useful example. Because Ticketmaster wished to preserve the value of its site to advertisers, Ticketmaster sought to prevent users from following "deep links" directly from Tickets.com's site to Ticketmaster's "interior" pages.[207] When a web browser contacts a server to retrieve a particular page, the browser conveys several pieces of information, including the contents of the "Referer" variable—a variable the user's browser typi-

robots.txt (last visited Aug. 20, 2004). For further discussion, see *infra* notes 382–85 and accompanying text. The CNN website provides an illustration of relatively detailed robots.txt instructions, with several specific robots disallowed from dozens of directories. *See* http://www.cnn.com/robots.txt (last visited Aug. 20, 2004).

[206] When a robot ignores the robots.txt instructions, a server owner may be able to detect that its site is being queried recursively. Even if she can detect the robot, she cannot modify her robots.txt file to exclude that particular robot unless the robot's developer has assigned it a unique user agent name—something that Hypertext Transfer Protocol version 1.1 (HTTP/1.1), the communications protocol currently used by web servers, permits but does not require. The robot exclusion standard is therefore effective only against "compliant" robots.

[207] *See supra* note 96.

cally sets to contain the address of the previously accessed web page.[208] The Referer variable benefits web server owners in a number of ways, by allowing the server to identify pages with links to the server, to trace obsolete or mistyped links, and to optimize caching.[209] For a site owner wishing to prevent deep linking, knowing the contents of the Referer variable allows the server owner to restrict access to certain files on the basis of the referring page and/or redirect users to the website's homepage. In other words, the site owner can allow or disallow access based on the site or page most recently visited by the user. Although reliance on the Referer variable allows a site owner to redirect some traffic to the main page, the site owner's control is not complete. The Referer variable can be "spoofed" to make it appear that the referring site was a trusted site when in fact it was not.[210] Tickets.com apparently exploited this fact to defeat Ticketmaster's efforts to block deep links.[211]

There are other technical measures a network resource owner can use to control access to her server. She may, for example, allow or deny access based on the network identity of the "host"—that is, the computer that originates the request for a web page. The server owner simply creates a file in the directory where the files to which the owner wishes to control access are located, and specifies, by domain name or IP address, which hosts are allowed or denied access to the files.[212] If a website owner wishes to block the use of robots, for example, she may be able to detect the IP address of a computer that is transmitting recursive data requests, and may then configure her system to block queries originating from that IP address. eBay used this approach in attempting to block Bidder's Edge's recursive que-

---

208 "Referer" is a misspelling of referrer. *See* R. Fielding et al., Hypertext Transfer Protocol—HTTP/1.1 Request for Comments 2616, § 14.36, at 86, *at* http://www.faqs.org/ftp/rfc/rfc2616.pdf (1999).

209 *Id.*

210 A simple Internet search reveals multiple sites discussing how to spoof the Referer variable.

211 *See* Ticketmaster Corp. v. Tickets.com, Inc., No. 99 CV-7654, 2000 WL 1887522, at *2 (C.D. Cal. Aug. 10, 2000) (discussing Ticketmaster's inability to block deep linking); Appellants' Opening Brief at 12 n.9, Ticketmaster Corp. v. Tickets.com, Inc., 2 Fed. Appx. 741 (9th Cir. 2001) (No. 00-56574) (explaining that Ticketmaster "attempted to block Tickets.com's deep-links, but Tickets.com circumvented those blocks the very same day"). Neither the district court opinion nor Ticketmaster's brief on appeal specifies that Tickets.com spoofed the Referer variable, but that is the most likely basis for Ticketmaster's inability to block the deep links.

212 For one of many server guides explaining access control options, see, for example, iPlanet Web Server, Enterprise Edition Administrator's Guide, Chapter 8: Controlling Access to Your Server, *at* http://docs.sun.com/source/816-5691-10/esaccess.htm (last visited Aug. 20, 2004).

ries,[213] and Intel also sought to block Hamidi's e-mails on this basis.[214] When a system relies solely on host authentication as a means of access control, however, it is vulnerable to IP address spoofing—that is, to the intentional misrepresentation of a source IP address to conceal the sender's identity or to impersonate a trusted computer system.[215]

Finally, a system owner can control access to an information server through some combination of username and password authentication. Such an approach is the most effective technical means of controlling access, but it is the most costly to maintain and gives the system owner the least flexibility.

There also may be a blurring between the code-based and commons approaches, depending on what sort of "commons" rule the law reflects. As noted earlier, I use the "commons" label to describe circumstances in which a system owner lacks the right to enjoin unwanted uses, irrespective of the notice she provides or the technical measures she employs. There are really two different types of "commons" rules, and they can result in quite different levels of access. Under one rule, which I label the "pure" liability rule, the law simply does not intervene to back a system owner's efforts to limit access. Even if a system owner attempts to use technical measures to block access, she is not entitled to an injunction to enforce those measures. Under the other rule, which I label the "technology displacing" rule, the law actually restricts the technical measures that a system owner could use to close access. The pure liability rule might lead to roughly the same level of access as an approach that requires a system owner to use a very strong technical measure in order to trigger the legal right to block unwanted uses. Under either the "strong" code-based approach or the pure liability approach, what kind of technical measure the system owner employs will determine the openness of a system. A brief example will explain why. If a system owner chooses a weak technical measure (such as using host authentication to block access from IP addresses suspected of robotic activity), access will nonetheless remain open to some users: under the code-based approach because the law does not back weak technical measures, and their circumvention is permissible; and under the pure liability approach because the law does not back technical measures at all. If the system owner chooses a strong technical measure (such as pass-

213 *See supra* note 96 and accompanying text.

214 *See supra* note 95 and accompanying text.

215 *See, e.g.*, CERT Advisory CA-1995-01, IP Spoofing Attacks and Hijacked Terminal Connections, *at* http://www.cert.org/advisories/CA-1995-01.html (last visited Aug. 21, 2004).

word protection), most access will be blocked. The difference is that under the code-based approach, those who have the technical ability to gain access may not do so because the law blocks such conduct, while under the pure liability approach, circumvention of even the stronger technical measure is permissible.

The situation is quite different for the technology-displacing rule. Because various types of technical measures are displaced under such an approach, the resulting level of access likely will exceed what would exist under the code-based or pure liability approaches. Indeed, the technology-displacing rule is the only one that actually would result in an open-access regime.

C. *Regulatory Effects of Law and Code*

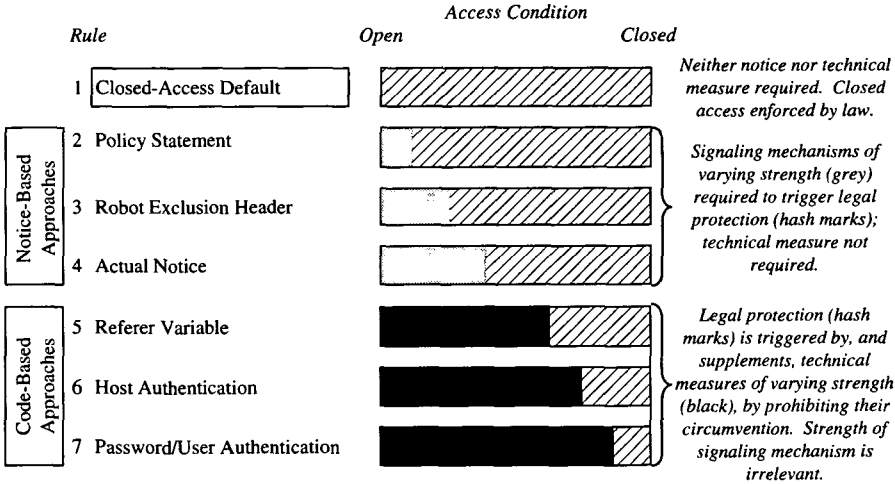
I have thus far focused mainly on the *legal* components of a system owner's efforts to control unwanted uses of network resources. As the discussion makes clear, however, legal measures are not the only kind of measures on which system owners can rely to control access. We have seen that system owners have a range of technical options as well. I discussed those measures above in terms of whether system owners had to use them to take advantage of legal protection, but it should be obvious that system owners can achieve varying degrees of protection through technical measures alone. The degree to which a system owner controls access thus depends on the combined effects of legal and technical measures. A few examples illustrate the point. To maximize a system owner's control over uses of his or her system, the law might proceed from a closed-access default and allow a system owner to block unwanted uses, even without providing notice of limitations on use of the system. With such strong legal protection, the system owner could achieve a closed-access condition—that is, block any and all unwanted uses—by operation of the legal rule alone. If we do not choose such a strong legal rule, the system owner might still be able to achieve the same degree of control by using technical mechanisms to control access (assuming the law allows for those technical mechanisms and provides an injunctive remedy if they are circumvented). Thus, by employing technical mechanisms, supplemented by law, a system owner could achieve access control nearly equivalent to the strongest legal rule.

Figure 1 represents this point schematically for the various approaches we have considered thus far. For each legal approach described in Sections A and B (except the commons approach), the figure shows how a system owner might combine legal and technical protection to achieve a closed-access condition—that is, full control

over unwanted uses over her system. The grey blocks signify the strength of the signaling mechanism necessary to trigger legal protection under various notice-based approaches, whereas the black blocks represent the strength of the technical measures necessary to trigger legal protection under various code-based approaches. The hash marks represent the legal protection necessary to achieve a closed-access condition; the greater the size of the hashed area, the greater the gap that must be filled by legal protection. Under each of the approaches, if the law recognized and backed up the validity of the mechanism, the system owner could, by utilizing that mechanism, control access to her system. (Because Figure 1 represents only those rules under which a system owner is entitled to injunctive remedy to control access, I defer illustration of the commons-based approaches, under which injunctive relief to control access is unavailable.)

As the figure illustrates, there are a number of different ways to achieve particular regulatory outcomes—through strong legal protection in the absence of any technical measure, through a strong technical measure supplemented by a relatively weak legal rule, and many possible approaches in between.

FIGURE 1
POSSIBLE REGULATORY OUTCOMES ACHIEVED BY LEGAL RULES AND TECHNICAL MEASURES



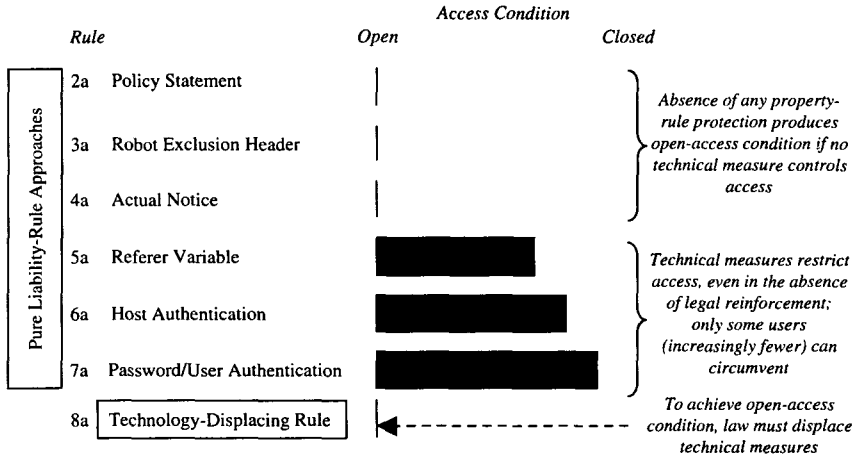
A second point about the relationship between law and code in producing regulatory outcomes emerges from Figure 1. If strong technical mechanisms are nearly as effective as legal protection, then system owners will still be able to achieve certain regulatory outcomes

even when we reject strong legal protection. Put another way, because system owners will always have the option to use technical mechanisms to block access, even a conclusion that a system owner should have no legal right to enjoin unwanted uses will not necessarily lead to open access. Figure 2 below illustrates the level of access control a system owner would have under the "commons" approaches—that is, if the law afforded a system owner no right to enjoin unwanted uses of her network resources. Attempting to signal limitations on permissible uses of the system would have no effect on access because the law would not enforce those limitations. Even under a pure liability-rule approach, however, a system owner would still have some control because she could use technical measures to block access: the stronger the technical mechanism, the closer a system owner would come to achieving full control over uses of her system. There would always be some users who could circumvent the technical measures and thus gain access, but fewer and fewer users would be able to do so as the technical measures became stronger. The possibility of circumvention means that a system owner's control over access is incomplete. Nevertheless, because technical measures are available, a pure liability approach would not lead to open access. To achieve a true open-access condition, the law would have to displace technical measures that would otherwise block access; in other words, a technology-displacing rule (as represented by Rule 8a in Figure 2 below) would be required.

D. Property and Liability Rules Revisited

Taken together, Figures 1 and 2 illustrate that, in considering from a normative perspective how the law should protect a network resource owner's right to control unwanted uses, we do not face a simple, binary choice between property rules and liability rules. Rather, we actually have a complex array of legal rules from which to choose. Returning to Figure 1, the legal rule proceeding from a closed-access default presumption (illustrated as Rule 1) provides the system owner with property-rule protection in all circumstances: It would allow a system owner to enjoin all unwanted uses of her system, even if she neither alerts potential users in advance of the scope of permissible uses nor actually tries to block unwanted uses. The legal rules that would give a system owner the right to enjoin unwanted uses of her system so long as she appropriately signaled the permissible uses of that system (illustrated as Rules 2, 3, and 4 in Figure 1) do provide property-rule protection, but they also reflect a feature of liability rules: Access is open unless and until the system owner pro-

FIGURE 2
POSSIBLE REGULATORY OUTCOMES IN ABSENCE OF PROPERTY-RULE PROTECTION



vides the notice specified by each rule. In other words, until the system owner provides adequate notice, the only remedy for unwanted access would be damages for certain harms caused (liability-rule protection). The provision of notice, however, would trigger an opportunity for the system owner to enjoin unwanted access (property-rule protection).

Similarly, the legal rules that would give a system owner the right to block unwanted uses of her system so long as technical mechanisms provide an appropriate level of actual control over uses of the system (illustrated as Rules 5, 6, and 7 in Figure 1) have both liability-rule and property-rule features. Unless and until a technical measure blocks access, access is open, with the system owner's sole remedy being damages for harms caused. If the system owner employs a sufficiently strong technical measure, however, she can rely on the law to enjoin uses that evade those controls.

All of these hybrid liability/property rules approaches might appropriately be described as "loperty" rules—a term that Abraham Bell and Gideon Parchomovsky have used to describe liability rules that spring into property rules when certain conditions are met.[216] With respect to all of these hybrid rules (Rules 2–7 in Figure 1), the default is a zero-order liability rule—that is, access is permitted, and the price of access is set at zero.[217] Once the system owner meets the

216 *See* Bell & Parchomovsky, *supra* note 101, at 53.
217 *See id.*

requisite condition, by signaling restrictions on access (for Rules 2–4) or blocking access with a mechanism of appropriate strength (for Rules 5–7), the law restores to the system owner the right to dictate the terms of access. In identifying the "loperty" rule as a form of legal protection, Bell and Parchomovsky provide the example of "fencing out" statutes that governed ranging property in the United States in the 1800s,[218] and that still apply in certain states.[219] Rather than applying the English common-law rule that prevented cattle from grazing on a neighbor's land, the fencing-out rule permitted cattle to roam freely on others' property until the property owner erected a fence meeting certain specifications.[220] Once the landholder erected the fence, "the landholder could exclude cattle grazers by means of injunction, and could collect damages in the event of a trespass."[221] Note the similarities between the fencing-out rule and code-based approaches to server access: The use of an appropriate technical mea-

---

218 *Id.* at 53–54; *see, e.g.*, Buford v. Houtz, 133 U.S. 320, 328 (1890) ("It has never been understood that in [sparsely populated] regions [of] this country . . . a man was bound to keep his cattle confined within his own grounds, or else would be liable for their trespasses upon the unenclosed grounds of his neighbors."). As the *Buford* court recognized: "Such a principle was ill-adapted to the nature and condition of the country at that time." *Id.* Although the "fencing out" rule is often presumed to have predominated only in western states, during the nineteenth century a number of northern and eastern states adopted that rule as well. *See* Robert C. Ellickson, *Of Coase and Cattle: Dispute Resolution Among Neighbors in Shasta County*, 38 STAN. L. REV. 623, 660 n.94 (1986); Coby Dolan, Comment, *Examining the Viability of Another Lord of Yesterday: Open Range Laws and Livestock Dominance in the Modern West*, 5 ANIMAL L. 147, 157 (1999).

219 Arizona, Colorado, Idaho, Montana, New Mexico, Texas, Utah, Washington, and Wyoming all have some form of open-range provision, in some cases permitting municipalities to create herd districts in which fence-in rules apply. *See* ARIZ. REV. STAT. ANN. § 3-1427 (West 2002) (prohibiting recovery of damages resulting from animal trespass unless land is enclosed within lawful fence, except in no-fence districts); COLO. REV. STAT. § 35-46-102(1) (2003) (allowing recovery if livestock breaks through lawful fence in good repair); IDAHO CODE § 25-2118 (Michie 1990) (defining open range as "uninclosed lands outside of cities, villages and herd districts, upon which cattle by custom, license, lease, or permit, are grazed or permitted to roam"); *id.* § 25-2401 (allowing creation of herd districts in which open-range doctrine does not apply); MONT. CODE ANN. § 81-4-203 (2003) (defining "open range"); *id.* § 81-4-215 (allowing recovery if, outside of herd district, animal breaks through lawful fence and owner of animal was negligent); N.M. STAT. ANN. § 77-12-5 (Michie 1999) (allowing recovery of damages for trespass within designated herd law district); *id.* §§ 77-16-1, -3 (requiring persons with "lands or crops that would be injured by trespassing animals" to use lawful fencing and requiring that landowners have appropriate fencing in order to recover for trespass committed by animals); TEX. AGRIC. CODE ANN. § 143.082(a) (Vernon 2004) (imposing liability for permitting livestock to run at large in county with range restrictions); UTAH CODE ANN. § 4-24-10(1)(a) (2003) (requiring livestock foraging on open range or outside enclosure to bear brand); WASH. REV. CODE ANN. § 16.60.015 (West 1992) (imposing liability for damages for trespass on land if fence is in good repair); WYO. STAT. ANN. § 11-28-108 (Michie 2003) (imposing liability if animal breaches lawful enclosure).

220 Bell & Parchomovsky, *supra* note 101, at 53.

221 *Id.*

sure that actually blocks some access is the triggering event that transforms the regime from a zero-order liability-rule baseline to a property rule; the difference between Rules 5, 6, and 7 in the illustration is that a different technical measure (of increasing strength) would be required under each rule to trigger the property-rule protection. Similarly, under the notice-based approaches, it is the use of an appropriate signaling measure that triggers property-rule protection; the difference between Rules 2, 3, and 4 in the illustration is that different signaling mechanisms (of increasing strength) would be required under each rule to trigger the property-rule protection.

Returning to Figure 2, we see that the matter is still more complicated. Even if we reject all of the approaches that involve the possibility of injunctive relief to block unwanted uses, it is not clear that open access will result. In the absence of sufficient legal protection, a system owner might use stronger technical protection. Some users may be able to circumvent the technical protection, but some will not. In other words, even if we remove the property owner's ability to use the threat of an injunction to dictate the terms of access by embracing a pure liability rule, the system owner still has the ability to use technical measures to restore her control—at least as to those who cannot circumvent. If the law is to achieve the desired level of open access, more than a liability rule may be required: The law must actually displace technical measures.

The observation that technical measures can supplement or supplant legal measures is not a new one. Scholars have made a similar point with respect to copyright law, observing that digital rights management systems allow copyright holders to appropriate greater protection than copyright law itself allows.[222] In addition, scholars have observed in other contexts that computer "code" can produce regulatory effects similar to law.[223] These points, however, have not been brought to bear on the cyberproperty debate, which seems to presume that an absence of legal protection will translate into open access.

It is especially important to consider the relationship between law and technology in the cyberproperty context because doing so reveals an important facet of that relationship that has largely been overlooked. System owners do not select technical measures in a legal vacuum. The choice of a particular *legal* rule can influence a system owner's choice of a *technical measure* to control access.[224] Consider,

---

222 *See supra* notes 133–36 and accompanying text.

223 *See infra* notes 391–407 and accompanying text.

224 Professor Polk Wagner makes a similar argument in a forthcoming article. *See* R. Polk Wagner, *On Software Regulation*, 78 CAL. L. REV. (forthcoming 2005), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=582422.

for example, a website that wishes to block robots. If the law does not allow the site owner to enjoin robotic activity that disregards either the owner's robot exclusion directives or her provision of actual notice that the robotic activity is unwanted, then the site owner must turn to some technical measure, such as attempting to block the source of the robotic activity altogether. In the absence of legal protection, system owners can simply strengthen their technical measures in an attempt to achieve the equivalent effect.

This analysis refines our inquiry into how the law should protect network resources. The choice is not merely between property-rule and liability-rule approaches, but between a property rule based on a default of closed access; two classes of rules perhaps best described as "loperty" rules because of the necessity for some event to trigger property-rule protection; a liability rule that would accept the existence of some technical mechanisms to block access, even though those technical mechanisms could in many cases prevent achievement of an open-access condition; and a rule that displaces technical mechanisms that block access (i.e., a technology-displacing rule). In weighing the choice among these possible approaches, moreover, it is important to keep in mind that the selection of a too-weak legal rule may prompt greater reliance on technical measures. With these refinements in place, the next Part examines the current state of the law and which of these approaches is most appropriate for protecting network resources.

III
RETHINKING CYBERPROPERTY CLAIMS

In this Part, I draw upon the more complete framework of Part II to explain current legal approaches to protection of network resources and to consider what legal approaches are most preferable. Section A shows that the problem with current case law is that courts have drifted toward a default presumption of closed access. That trend has resulted from a flawed reading of the early Internet trespass cases, such as *CompuServe* and *eBay*. The early case law, I argue, actually reflects a "loperty" rule approach to protection of network resources—it is consistent with a default presumption of open access, where a system owner then takes certain steps (either notice-based or code-based) to trigger property-rule protection. In Section B, I argue that courts must curtail this drift toward a closed access approach.

Section C considers the more difficult choice among notice-based, code-based, and commons approaches. Analyzing the Computer Fraud and Abuse Act (CFAA), I argue that, as a doctrinal matter,

courts should only validate technical restrictions on access. For other cyberproperty claims, the issue is normative rather than doctrinal. In weighing the relevant normative considerations, I focus both on the degree of open access that different rules are likely to produce and on the relative balance of legal protection and technical protection. Because technical measures lack the flexibility of legal measures and have uneven effects on users, the balance between technical and legal measures is important. The relative effects of technical and legal measures should lead us to favor legal protection over technical protection. A pure liability-rule approach or a code-based approach requiring strong technical measures is likely to induce greater reliance on technical measures to mimic property-rule protection. As a result, the law should neither deny injunctive relief for unwanted access nor require a system owner to employ strong technical measures to trigger a right to injunctive relief. As long as courts proceed from a default assumption of open access and place the burden on the system owner to clearly convey the contours of permissible use, property-rule protection should prevail.

A. Current Legal Approaches

In this Section, I explore the various legal doctrines network resource owners have invoked to block unwanted uses of their systems. For trespass-to-chattels claims and claims under the CFAA, a distinctive pattern emerges. Cases raising these claims under the CFAA typically involve requests for injunctive relief against defendants who had actual notice of the plaintiff's objection to the conduct in question but refused to cease their activity. Courts have allowed actual notice to trigger a plaintiff's legal right to block unwanted uses of her system. In other words, under trespass doctrine and the CFAA, courts have taken an approach consistent with Rule 4 in Figure 1. But broader pronouncements in these cases suggest that far weaker notice mechanisms might also be sufficient to trigger a legal right to block unwanted uses. In particular, courts have stated that activities inconsistent with policy statements or terms of use posted at some location on a network are sufficient to trigger liability under trespass-to-chattels doctrine and the CFAA. Because courts have not evaluated whether the policy statements or terms of use are likely to give users actual notice of limits on use of the system, or whether users agreed to the terms, this approach has the potential to produce results very close to those produced by a default rule of closed access. The legal protection for network resources that this approach affords—close to that depicted as Rule 2 in Figure 1—has liability-rule and property-rule

components, but it takes very little for the system owner to trigger property-rule protection. Courts considering contract claims have more explicitly assessed whether users had notice of and assented to terms of use purporting to set forth permissible uses of a system. Despite this more explicit analysis, courts have tended to find enforceable the same sorts of weak signaling mechanisms that have provided the basis for trespass-to-chattels and CFAA claims.

Although a number of courts have drifted toward a default rule of closed access, a handful of courts have rejected the view that even strong forms of notice can trigger a system owner's right to enjoin activities inconsistent with that notice.[225] Because those cases also involved certain (weak) technical measures designed to block some access, courts' denial of injunctive relief implicitly suggests that even (weak) code-based controls would not trigger a right to enjoin unwanted uses. I examine trespass-to-chattels, CFAA, and contract claims in turn.

1. Trespass to Chattels

As discussed earlier, to sustain a trespass-to-chattels claim in the case of network resources, a plaintiff must show that the defendant intentionally interfered with the plaintiff's possessory interest in personal property, by "using or intermeddling with" the property.[226] The defendant's conduct, of course, must be without the plaintiff's consent. As I will show, several successful trespass-to-chattels cases involved requests for injunctive relief when a defendant had actual notice of the plaintiff's objection to the conduct in question. Courts in such cases have thus allowed system owners to exclude unwanted uses when they have provided strong signals that the use is unwanted. On a handful of occasions, however, courts have assumed or held that policy statements or terms of use posted on the network are sufficient to establish the range of permissible uses of the system, without any inquiry into whether users had notice of or assented to the relevant terms. Such an approach is dangerously close to a default presumption of closed access.

a. Actual Notice Cases

One of the central premises of the case that launched the electronic trespass line, *CompuServe Inc. v. Cyber Promotions, Inc.*,[227]

---

225 *See infra* Part III.A.1.c.

226 RESTATEMENT (SECOND), *supra* note 24, § 217; *see also supra* note 24 and accompanying text.

227 962 F. Supp. 1015 (S.D. Ohio 1997).

was that even though CompuServe had connected its servers to the Internet, Cyber Promotions's transmission of e-mail to those servers was without CompuServe's authority.[228] The court concluded that CompuServe had specifically notified Cyber Promotions that its messages were unwelcome,[229] and that whatever consent CompuServe might have conveyed by opening its mail servers was thereby limited or revoked. Other bulk e-mail cases have followed this approach. In *America Online, Inc. v. IMS*, for example, a district court held a bulk e-mailer liable for trespass when the e-mailer continued to transmit e-mail after receiving a cease-and-desist letter.[230] Similarly, the lower court's decision in *Intel Corp. v. Hamidi* observed that Intel instructed Hamidi to stop sending messages to Intel's employees through Intel's mail server.[231] Cases involving websites reflect a similar analysis. In *eBay, Inc. v. Bidder's Edge, Inc.*, for example, in finding that Bidder's Edge made unauthorized use of eBay's system, the court relied in part on eBay's explicit notification to Bidder's Edge that its actions were unauthorized.[232]

In holding that explicit notice is sufficient to indicate that a system owner does not consent to particular uses, and thus to trigger a system owner's right to enjoin such uses, these cases are unremarkable, and they produce a legal rule for protecting network resources consistent with Rule 4 in Figure 1. Before proceeding further, however, we should consider an alternative, narrower reading of the cases. In all three cases—*CompuServe*, *eBay*, and the lower court *Hamidi* decisions—the courts noted that the system owners sought to block the defendants' activities through technical measures.[233] It might thus be argued that the courts sustained the plaintiffs' trespass claims not because the plaintiffs supplied notice of their objections, but because

---

228 *Id.* at 1024; *see also supra* note 27 and accompanying text.

229 *CompuServe*, 962 F. Supp. at 1024.

230 24 F. Supp. 2d 548, 550 (E.D. Va. 1998).

231 114 Cal. Rptr. 2d 244, 246, 250 (Ct. App. 2001).

232 100 F. Supp. 2d 1058, 1062, 1070 (N.D. Cal. 2000).

233 The *CompuServe* court observed that CompuServe had attempted to block receipt of Cyber Promotions' messages, but that Cyber Promotions had configured its computers "to conceal their true domain name and appear on the Internet as another computer." *CompuServe*, 962 F. Supp. at 1019. Although the court did not specify the particular screening procedure CompuServe implemented, the discussion of the procedure is consistent with host authentication—that is, screening communications in or out based on the IP address or domain name of the originating computer. In *eBay*, having identified Bidder's Edge's unauthorized robotic activity, eBay used host authentication to block queries from Bidder's Edge, but Bidder's Edge defeated that technology by relying on third-party proxy servers to disguise the origin of its data requests. *eBay*, 100 F. Supp. 2d at 1061–63. Similarly, Intel attempted to block transmission of Hamidi's messages, but Hamidi "us[ed] different sending computers" to evade the blocks. Intel Corp. v. Hamidi, 71 P.3d 296, 301 (Cal. 2003).

the plaintiffs in fact used *code-based* measures—albeit weak ones—to control access to their systems. In other words, rather than treating the cases as endorsing a notice-triggered injunction rule, we might view them instead as supporting a code-triggered injunction rule. The difficulty with this argument is that only one of the three courts—*CompuServe*—actually attached any legal significance to the plaintiff's use of technical measures, stating simply that "the implementation of technological means of self-help . . . is particularly appropriate . . . and should be exhausted before legal action is proper."[234] Even in *CompuServe*, the court did not suggest that notice-based measures were incapable of triggering legal protection or that technical measures provide a more appropriate trigger; rather, the court's point was that, if the system owner could successfully block unwanted communications through technical measures, an award of injunctive relief might be improper. *CompuServe*, *eBay*, and the lower court decisions in *Hamidi*, along with similar cases, are thus best read as holding that actual notice can trigger a system owner's right to exclude unwanted uses.

b. Policy Statements and Terms of Use

Although *CompuServe*, *eBay*, and the lower court decisions in *Hamidi* may be unremarkable insofar as they suggest that explicit notice is sufficient to trigger trespass liability, they do contain broader language suggesting that system owners also can rely on policy statements posted at some location on their networks to establish limits on access to their systems. The *CompuServe* court, for example, observed that CompuServe had a bulk e-mail policy stating that "CompuServe does not permit its facilities to be used by unauthorized parties to process and store unsolicited e-mail."[235] The court questioned whether that statement had been sufficiently communicated to third parties sending messages to CompuServe's mail servers,[236] but because it found that Cyber Promotions had actual notice of CompuServe's objection, the court did not need to resolve the issue. Similarly, the *eBay* court noted that eBay's user agreement prohibited the use of robots or crawlers.[237] Because eBay had specifically objected to Bidder's Edge's conduct, however, the court again did not

234 *CompuServe*, 962 F. Supp. at 1023.

235 *Id.* at 1024.

236 *Id.* ("It is arguable that CompuServe's policy statement, insofar as it may serve as a limitation upon the scope of its consent to the use of its computer equipment, may be insufficiently communicated to potential third-party users when it is merely posted at some location on the network.").

237 *eBay*, 100 F. Supp. 2d at 1060.

need to pass on whether activities inconsistent with eBay's user agreement were sufficient to establish Bidder's Edge's liability. Indeed, the court observed that the record did not indicate whether that agreement was in force at the time Bidder's Edge's robots began crawling the site, or whether Bidder's Edge ever manifested assent to it.[238]

Although *CompuServe* and *eBay* did not rest liability solely on activities inconsistent with policy statements, some decisions purporting to follow the reasoning of *CompuServe* and *eBay* have focused more heavily on such mechanisms. In these cases, many of the relevant restrictions appeared in terms of use that purported to bind subscribers, but the failure of the courts to inquire into issues of notice and assent indicates a willingness to permit weak forms of notice to trigger legal protection. In other words, by failing to inquire into issues of notice and assent, courts essentially converted user agreements into mere policy statements. In *America Online, Inc. v. LCGM, Inc.*, for example, the court found an e-mailer liable for trespass because the e-mailer's actions—harvesting e-mail addresses of AOL members and sending bulk e-mail to those members—violated AOL's terms of service and bulk e-mail policy.[239] The court noted in a footnote that AOL also premised its claim that the defendants' activities were unauthorized on the defendants' continued sending of bulk e-mail after receiving cease-and-desist letters from AOL.[240] The court did not, however, attach legal significance to the cease-and-desist letters. Similarly, in *Hotmail Corp. v. Van$ Money Pie Inc.*, the court premised the defendant's liability for trespass on its sending of spam from a Hotmail e-mail account, an activity that Hotmail's terms of service prohibited.[241]

In both *LCGM* and *Hotmail*, because the senders of the e-mails maintained accounts with the objecting service provider,[242] the courts could have inquired whether the terms of service were presented in such a way as to give the subscribers sufficient notice of the restrictions or whether the subscribers agreed to those terms. The courts did not engage in this sort of analysis, instead assuming that any activities inconsistent with the service providers' announced policies would

---

238 *Id.*

239 Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998).

240 *Id.* at 452 n.4.

241 Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020, 1025 (N.D. Cal. 1998).

242 *See LCGM*, 46 F. Supp. 2d at 448 (observing that bulk e-mailers were AOL members); *Hotmail*, 47 U.S.P.Q.2d (BNA) at 1021 (finding that e-mailers maintained Hotmail accounts).

trigger liability.[243] One could argue that the plaintiff's filing of a suit for injunctive relief necessarily provides the defendant with notice that the system owner objects to the defendant's use; if continued use of the system by the defendant constitutes unauthorized use for purposes of a trespass claim, then the contents of the system owner's terms of use or policy statements ought to be irrelevant to the inquiry.[244] In *LCGM*, however, the court focused on AOL's terms of service and the bulk e-mail policy not only as a basis for injunctive relief to prevent further trespasses, but also as a basis for damages for past activities (apparently including activities that pre-dated AOL's sending of the cease-and-desist letter).[245] That approach necessarily depended on the conclusion that breach of policies limiting use of a system can form the basis for a trespass claim. In focusing heavily on policy statement–based limitations, the courts adopted an approach close to that reflected in Rule 2 in Figure 1.[246]

c. Cases Rejecting Trespass Claims

Although most courts have allowed actual notice, or weaker forms of notice, to trigger a system owner's right to block unwanted uses, two courts—the district court in *Ticketmaster Corp. v. Tickets.com, Inc.*[247] and the California Supreme Court in *Hamidi*[248]—?have explicitly rejected that approach. *Ticketmaster*, like *Com-*

---

[243] *See LCGM*, 46 F. Supp. 2d at 452 ("Because AOL's Unsolicited Bulk E-mail Policy and Terms of Service prohibit the sending of such e-mails, defendants' actions were unauthorized."); *Hotmail*, 47 U.S.P.Q.2d (BNA) at 1025 ("[D]efendants intentionally trespassed on Hotmail's property by knowingly and without authorization creating Hotmail accounts that were used for purposes exceeding the limits of the Terms of Service . . . .").

[244] *Cf.* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000) (concluding, for purposes of applying federal prohibition on unauthorized access to computer system, that "it is clear since at least the date this lawsuit was filed that Register.com does not consent to Verio's use of a search robot, and Verio is on notice that its search robot is unwelcome"), *aff'd*, 356 F.3d 393 (2d Cir. 2004).

[245] The court did not award damages at the summary judgment phase because the amount of damages presented a question of fact. *LCGM*, 46 F. Supp. 2d at 552. In recognizing that damages would be appropriate, however, the court obviously rested its conclusion that LCGM's conduct was unauthorized on something other than the notice provided by AOL's filing of the lawsuit, for that notice could have supported only an injunctive remedy. Moreover, in discussing LCGM's liability, the court drew no distinction between conduct pre-dating and post-dating AOL's cease-and-desist letters. *See id.* at 452 & n.4 (focusing on defendants' violation of terms of service and mentioning, without further discussion, AOL's allegations that cease-and-desist letters "further demonstrated" that defendants' conduct was unauthorized).

[246] I discuss the doctrinal and normative implications of this approach in Part III.B, *infra*.

[247] Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).

[248] Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).

puServe and *eBay*, involved actual notice to Tickets.com that Ticketmaster objected both to Tickets.com's use of robots to recursively query Ticketmaster's site and to Tickets.com's use of "deep links" to Ticketmaster's internal pages.[249] In denying Ticketmaster's trespass claim, the district court rejected the notion that actual notice of unwanted activities could trigger Ticketmaster's right to exclude unwanted uses.[250] Similarly, in *Hamidi*, the California Supreme Court did not view Intel's actual notice to Hamidi of limitations on use of its system as a sufficient basis for injunctive relief.[251] Both *Ticketmaster* and *Hamidi*, then, reject the approach reflected in Rule 4 of Figure 1.

Because both cases also involved the evasion of technical measures designed to thwart the defendants' activities, we might also view those cases as implicitly rejecting the possibility that (weak) code-based mechanisms can trigger a right to injunctive relief. Ticketmaster unsuccessfully sought to block queries from Tickets.com's robots[252] and to redirect traffic from its interior pages to its main pages.[253] Although the court did not discuss the significance of Ticketmaster's technical efforts to block recursive queries and deep linking, its conclusion that Ticketmaster could not sustain a trespass claim at least implicitly suggests that evasion of the particular code-based mechanisms Ticketmaster used in an attempt to control access—presumably host authentication for robots and restrictions on referring sites via the Referer variable—could not trigger a right to exclude unwanted uses. Similarly, although the *Hamidi* court noted that Intel had attempted to block Hamidi's messages,[254] the court did not discuss the significance of Hamidi's evasion of Intel's measures. Whether that evasion involved "spoofing" the IP address of the computer from which Hamidi sent messages or actually switching computers is unclear from the facts of the case. Under an approach allowing implementation of code-based controls on access to trigger a system owners' legal right to exclude unwanted access, that distinction might well matter because a court might consider only the spoofing to

---

[249] *Ticketmaster*, 2003 WL 21406289, at *2 (indicating that Tickets.com was familiar with Ticketmaster's terms of use and that Ticketmaster had made its objections clear in letter to which Tickets.com responded).

[250] *Id.* at *3 (granting summary judgment to Tickets.com on trespass claim); Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 WL 1887522, at *4–*5 (C.D. Cal. Aug. 10, 2000) (denying preliminary injunctive relief).

[251] *Hamidi*, 71 P.3d at 301, 311 (denying trespass claim in spite of Intel's explicit demand that Hamidi stop sending e-mails to Intel's system).

[252] *Ticketmaster*, 2003 WL 21406289, at *3 (noting Ticketmaster's efforts to "frustrate" Tickets.com's spider).

[253] *Ticketmaster*, 2000 WL 1887522, at *2 (discussing Ticketmaster's thwarted efforts to redirect traffic from its interior pages to its main pages).

[254] *Hamidi*, 71 P.3d at 301.

constitute circumvention of the technical measure. In rejecting Intel's trespass claim, however, the *Hamidi* court did not discuss the issue, and thereby implicitly rejected an approach under which a (weak) code-based access control would trigger trespass liability. The *Ticketmaster* and *Hamidi* courts thus implicitly rejected approaches such as those reflected in Rules 5 and 6 of Figure 1.

In sum, although courts considering trespass claims have relied on system owners' specific objections as a basis for enjoining unwanted contacts, several courts have also suggested or assumed that policies posted on the network can adequately signal limitations on use of a system. For the most part, courts have not considered whether any policy statements or terms of use are reasonably calculated to give users notice of permissible uses, or whether users assented to the relevant terms. These approaches pave the way for adoption of a legal rule that requires only weak signaling mechanisms to trigger a system owner's right to exclude unwanted uses. Even though some of the cases also involved technical measures designed to block access, courts did not rely on evasion of these technical measures as the basis for enjoining the defendants' conduct. Finally, a handful of courts have rejected trespass claims, even though the defendants had actual notice of objections to their use of the systems and evaded technical measures to gain access. I depict the courts' positions schematically, along with those of courts considering CFAA and contract claims, in Figure 3 (found in Part III.A.4).

2. *The Computer Fraud and Abuse Act*

In addition to raising trespass claims, plaintiffs objecting to unwanted uses of their systems have increasingly brought civil claims under the federal computer crime statute, often referred to as the Computer Fraud and Abuse Act.[255] As in the trespass context, civil claims under the CFAA were first brought in an attempt to curtail unwanted bulk e-mail. Courts later applied the statute to disputes over recursive queries. As in the trespass context, most of the claims have involved injunctive relief in circumstances in which a defendant has actual notice of the plaintiff's objection to her activities. Courts have nevertheless assumed that violations of the CFAA can be predicated on a range of activities, including access to a computer system in violation of policy statements purporting to outline the permissible

255 18 U.S.C.A. § 1030 (West 2000 & Supp. 2004). Technically, the title Computer Fraud and Abuse Act refers to the 1986 amendments to 18 U.S.C. § 1030, *see* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213–16, but courts commonly use it to describe 18 U.S.C. § 1030 as a whole.

uses of a system. Courts' application of the CFAA in this context has thus produced a body of federal law that closely parallels cases based on state law trespass-to-chattels claims.

The CFAA criminalizes certain conduct with respect to a "protected computer," defined to include any computer "used in interstate or foreign commerce or communication."[256] In 1994, Congress amended the statute to provide a civil cause of action for injunctive relief or damages when the challenged activities cause "damage" or "loss."[257] Most of the CFAA's provisions prohibit unauthorized "access" to a protected computer,[258] coupled with some other conduct. Unauthorized access can take one of two forms. First, a defendant might have authority to engage in certain activities with respect to a computer system, but he might "exceed" that authority. The statute defines "exceed[ing] authorized access" as: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[259] Second, a defendant might have no authority whatsoever to gain access to a computer system; any access would be "without authorization." The statute does not define that phrase, nor does it define the term "access." Several of the criminal provisions of the statute require only "access without authorization,"[260] while other provisions target both "access without authorization" and "exceed[ing] authorized access."[261]

---

256 18 U.S.C. § 1030(e)(2)(B) (2000 & Supp. I 2001).

257 Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001(d), 108 Stat. 1796, 2098 (codified as amended at 18 U.S.C. § 1030(g) (2000 & Supp. I 2001)).

258 The exceptions are § 1030(a)(5)(A)(i), which prohibits one from knowingly transmitting "a program, information, code, or command, and as a result of such conduct . . . caus[ing] damage without authorization, to a protected computer"; § 1030(a)(6), which prohibits trafficking in an access code or password; and § 1030(a)(7), which prohibits transmitting a threat to cause damage to a protected computer for purposes of extortion.

259 18 U.S.C. § 1030(e)(6) (2000).

260 *See* 18 U.S.C. § 1030(a)(3), (5)(A)(ii)–(iii) (2000 & Supp. I 2001).

261 *See* 18 U.S.C. § 1030(a)(1)–(2), (4) (2000). The distinction has led defendants charged or sued under provisions referring only to access without authorization to argue that they in fact had authority to gain access to a computer system; they merely exceeded authorized access. In other words, defendants argue that provisions containing the "without authorization" language apply only to "outsiders"—those with no authority to gain access to the system—whereas provisions containing both phrases apply to "insiders" as well as "outsiders." The Second Circuit, however, rejected such an argument in *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), which involved transmission of a worm that caused significant damage to a number of computers. At the time, the CFAA did not have a prohibition equivalent to what is now § 1030(a)(5)(A)(i), which bars the transmission of a file that causes damage without authorization, regardless of whether the sender is authorized to access the system in the first place. More recently, courts have tended to accept the

Each provision of the CFAA requires some further showing. For our purposes, the two most relevant provisions are § 1030(a)(2)(C), which prohibits a party from intentionally accessing without authorization or exceeding authorized access to a computer *and thereby obtaining information from a protected computer*; and § 1030(a)(5)(A)(iii), which prohibits one from intentionally accessing a protected computer without authorization, *and as a result of such conduct, causing damage.*

As a cursory reading of the CFAA reveals, the crucial question in applying the statute to a network resource owner's efforts to curtail unwanted uses of her system is what it means for access to a system to be "without authorization" or to "exceed[ ]" what has been authorized. Is access unauthorized merely because it is inconsistent with permissible uses a system owner has outlined in a policy statement posted at some location on the network? Is access unauthorized if a system owner notifies a user that his actions are unwanted? Or must a system owner employ some sort of technical mechanism to block access—and if so, how effective must that mechanism be for its evasion to trigger liability under the statute? As in the trespass context, we can fruitfully examine this issue with reference to the rules represented in Figure 1. In this Section, I consider how courts have resolved this issue thus far. As in trespass cases, courts have veered towards a closed-access default, by taking an approach consistent with Rule 2 and giving effect to policy statements and terms of use without inquiry into issues of notice and assent.[262] I discuss the current state of the law under the CFAA here. I later argue that, under a proper interpretation of the CFAA, only breach of a code-based control on access should trigger liability.[263]

a. Bulk E-Mail Cases

Service providers challenging the activities of bulk e-mailers have invoked both the prohibition in § 1030(a)(2)(C) against extracting information and the prohibition in § 1030(a)(5)(A)(iii) against causing damage.[264] Claims under § 1030(a)(2)(C) are usually based on use of

insider/outsider distinction. *See, e.g., In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1370–71 (S.D. Fla. 2001).

262 I discuss the implications of courts' movement toward a closed-access default in Part III.B, *infra*.

263 *See infra* Part III.C.1.

264 Most cases were actually decided under the former § 1030(a)(5)(C), which contained language identical to that now appearing in § 1030(a)(5)(A)(iii). A 2001 amendment renumbered § 1030(a)(5)(A)–(C) as § 1030(a)(5)(A)(i)–(iii) and imported into § 1030(a)(5)(B) language substantially similar to that previously appearing in the definition of "damage" in § 1030(e)(8). *See* Uniting and Strengthening America by Providing Appro-

a service provider's system to acquire e-mail addresses in order to create a bulk e-mail recipient list.[265] For example, in *America Online, Inc. v. LCGM, Inc.*,[266] the defendants maintained AOL memberships and used software to harvest addresses of AOL subscribers, albeit from sources accessible to AOL users generally.[267] AOL's policy on unsolicited e-mail and terms of service prohibited use of AOL membership to harvest e-mail addresses.[268] The court found that the defendants' activities were therefore unauthorized for purposes of § 1030(a)(2)(C).[269] In other words, because AOL's policy and terms of service prohibited the harvesting of e-mail addresses, the defendants' use of AOL's system for that purpose constituted unauthorized access to a protected computer, by which the defendants obtained "information" in violation of the statute. Similarly, in *America Online, Inc. v. National Health Care Discount, Inc.*,[270] an AOL member collected addresses of other AOL members for the purpose of sending unsolicited commercial e-mail. AOL successfully claimed that the conduct violated its terms of service, and that the defendants therefore exceeded authorized access for purposes of § 1030(a)(2)(C).[271] Despite the fact that the primary defendants in both *LCGM* and *National Health Care Discount* were AOL members, who would have been required to agree to AOL's terms of service, the court did not focus on the defendants' knowledge of AOL's terms—essentially converting what purported to be a user agreement into a mere policy statement.

Both *LCGM* and *National Health Care Discount* also raised claims that the defendants had gained unauthorized access to AOL's system and had caused damage for purposes of § 1030(a)(5)(A)(iii).[272]

---

priate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 814(a), 115 Stat. 272, 382–83 (2001). To avoid confusion, I refer to § 1030(a)(5)(A)(iii) in the text, even with respect to those cases actually decided under former § 1030(a)(5)(C).

265 Recent federal legislation addressing unsolicited commercial e-mail contains similar language dealing more directly with the harvesting problem. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 5(b)(1)(A)(i), 117 Stat. 2699, 2708 (to be codified at 15 U.S.C. § 7704(b)(1)(A)(i)) (prohibiting sending of commercial message if sender has reason to know that recipient's e-mail address was obtained using "automated means from an Internet website or proprietary online service operated by another person," if such website or online service included certain limitations on use of e-mail addresses).

266 46 F. Supp. 2d 444 (E.D. Va. 1998).

267 *Id.* at 448.

268 *See id.*

269 *Id.* at 450.

270 121 F. Supp. 2d 1255 (N.D. Iowa 2000).

271 *Id.* at 1276.

272 *Id.* at 1272–75; *LCGM*, 46 F. Supp. 2d at 450–51.

The courts approached these claims in different ways, both on the issue of what "access" allegedly violated the statute and on the issue of when such access would be unauthorized. The *National Health Care Discount* court focused on the actual *sending* of the unsolicited commercial e-mail to AOL's system: If the transmission of e-mail to AOL's mail servers was unauthorized within the meaning of the statute, then that activity would trigger liability.[273] Section 1030(a)(5)(A)(iii), however, only covered "access without authorization," not "exceed[ing] authorized access." Since the primary e-mailer was an AOL member, the court was reluctant to conclude that he had sent e-mail "without authorization," even though he clearly had "exceed[ed] authorized access" in doing so.[274] Defendants other than the primary e-mailer were not AOL members, and the statute's prohibition on access without authorization therefore might have reached their conduct. Again, the court was wary, this time questioning whether AOL's policies on bulk e-mail could restrict the activities of non-members sending mail to AOL members.[275] Because the court imposed liability under § 1030(a)(2)(C), the court found it unnecessary to resolve these issues.[276]

The *LCGM* court took a different approach. Rather than analyzing the *sending* of unsolicited commercial e-mail to determine whether that activity constituted access without authorization that caused damage, the court again focused on the *harvesting* of e-mail addresses as satisfying the "access without authorization" predicate.[277] That unauthorized access, the court reasoned, enabled the defendant to send large quantities of unsolicited e-mail to AOL members, thereby causing damage to AOL's computer system, reputation, and goodwill.[278] Unlike the *National Health Care Discount* court, the *LCGM* court did not consider the possibility that liability under § 1030(a)(5)(A)(iii) should be confined to non-AOL members.

Taken together, *LCGM* and *National Health Care Discount* suggest that the extraction of e-mail addresses by subscribers in violation

---

273 121 F. Supp. 2d at 1273.

274 *Id.* at 1273 ("[I]t is not clear that a violation of AOL's membership agreements results in 'unauthorized access.' If AOL members are 'insiders' rather than 'outsiders' for purposes of section 1030(a)(5), then subparagraph [(A)(iii)] does not apply at all . . . ."); *see also* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 899 (N.D. Iowa 2001) (noting that additional development of record at trial did not clarify issue).

275 *Nat'l Health Care Disc.*, 121 F. Supp. 2d at 1273 (asking if "by imposing restrictions on its members, [AOL can] deny or restrict the rights of non-member Internet users with respect to sending any type or volume of e-mail to AOL members").

276 *Nat'l Health Care Disc.*, 174 F. Supp. 2d at 899.

277 *LCGM*, 46 F. Supp. 2d at 451.

278 *Id.*

of terms of service and other policy statements will constitute unauthorized access for purposes of § 1030(a)(2)(C), which targets the gathering of information. *National Health Care Discount* also suggests that, under § 1030(a)(5)(A)(iii), the sending of e-mail itself will constitute unauthorized access, creating a parallel to state-law trespass cases that have held that sending unwanted e-mail can constitute unauthorized use or intermeddling. *National Health Care Discount*, however, creates a potential outer limit on the reach of § 1030(a)(5)(A)(iii) by introducing the possibility that only an "outsider" can violate it, and that a violation must be based on something other than a policy statement or terms of service (which, the court implied, could not bind outsiders).

In both cases, of course, the e-mailers had actual notice of AOL's objection to their conduct because AOL sent cease-and-desist letters and ultimately sued.[279] To the extent that the cases involved injunctive relief, the courts need not have looked to terms of use or policy statements to signal limitations on use of AOL's system: If indeed extracting e-mail addresses from the AOL network constitutes "access" within the meaning of the CFAA, and if actual notice of an objection suffices to make that access unauthorized, the courts could have granted prospective relief based on AOL's objection alone. Both cases, however, also involved damages claims for conduct that pre-dated AOL's explicit notices, and in both cases the court found the defendants liable for damages.[280] As a result, AOL's terms of service and policy statements were necessary to the disposition of the cases: The notice that appears to have triggered legal protection came from those online documents.[281]

b. Automated Query Cases

Courts applying CFAA claims in cases involving automated or recursive queries have likewise given effect to online terms and found liability in circumstances analogous to those in trespass cases. In

[279] *Nat'l Health Care Disc.*, 174 F. Supp. 2d at 896; *LCGM*, 46 F. Supp. 2d at 448.

[280] In *LCGM*, the sending of unsolicited e-mail began approximately June 17, 1997, and AOL sent its first of two cease-and-desist letters on December 8, 1997. 46 F. Supp. 2d at 448. The *LCGM* court did not award damages at the summary judgment phase because the amount of damages presented a question of fact. *Id.* at 452. The opinion, however, in assessing liability, draws no distinction between LCGM's conduct before and after the cease-and-desist letters. *See id.* at 450–51. In *National Health Care Discount*, the sending of unsolicited e-mail began in the fall of 1997, *see* 121 F. Supp. 2d at 1263, and AOL sent its first cease-and-desist letter on July 1, 1998, *see* 174 F. Supp. 2d at 896. The court based its damage award on conduct occurring from 1997 through May 30, 1999. *See id.* at 896–97.

[281] Because the disputes involved subscribers, the courts could have looked to whether the terms of service were enforceable against subscribers as a matter of contract law. The courts did not, however, specifically inquire into the elements of notice and assent.

Register.com, Inc. v. Verio, Inc.,[282] a case raising trespass, CFAA, and contract claims, a domain-name registrar sought to enjoin Verio from using automated queries to gather information from its public database. To receive accreditation from the Internet Corporation for Assigned Names and Numbers (ICANN) as a registrar, Register.com was required to maintain a database of information about its registrants and to make that database available to the public.[283] Verio used a series of automated requests to extract information about Register.com's new registrants. Verio would then use the information to offer services to the new registrants—including some services in competition with those offered by Register.com itself.[284] Register.com claimed that Verio's automated queries to Register.com's system violated § 1030(a)(2)(C) and § 1030(a)(5)(A)(iii) of the CFAA.[285]

Register.com had terms of use, but those terms did not purport to restrict automated queries of its publicly available system.[286] The terms did, however, prohibit the *use* of information extracted from its database for purposes of sending unsolicited e-mail or making unsolicited phone calls.[287] Despite the fact that the terms of use were devoid of relevant restrictions on access to the computer system itself, the district court found Verio's access to Register.com's system unauthorized for purposes of § 1030(a)(2)(C)'s prohibition on gaining unauthorized access and thereby obtaining information. Prior to its access to Register.com's system, Verio knew that the data sought would be used for an unauthorized purpose;[288] that fact, the court reasoned, made its initial access to the system to acquire the data unauthorized.

Considering the claim under § 1030(a)(5)(A)(iii) that Verio's access without authorization had caused damage, the court simply held that Register.com's objection to Verio's activities—an objection

---

282 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004). The Court of Appeals did not address the CFAA claim on appeal, finding sufficient basis to affirm on the trespass and breach-of-contract claims. 356 F.3d at 406. The case is unusual in that it contains as an appendix an unadopted opinion drafted by Judge Fred I. Parker, a member of the court of appeals panel who died before the case was resolved. *See id.* at 394 n.*, 406. In the unadopted opinion, Judge Parker would have reversed the grant of injunctive relief on the CFAA and contract claims. *Id.* at 407. With respect to the CFAA claim, Judge Parker focused on Register.com's inability to meet the damage threshold, not the district court's application of the substantive standard. *Id.* at 440.

283 *Register.com*, 126 F. Supp. 2d at 241–42.

284 *Id.* at 243.

285 *Id.* at 251.

286 *Id.* at 249 (stating, in context of trespass-to-chattels claim, that "the Court does not believe that Register.com's terms of use forbid the particular use of the search robot at issue here").

287 *Id.* at 242.

288 *Id.* at 253.

made clear by Register.com's filing suit—rendered any further access by Verio unauthorized.[289] On the basis of Register.com's claim that Verio's activities, if replicated by others, would diminish its server capacity and slow its system, the court concluded that Register.com was entitled to preliminary injunctive relief. Apart from the fact that the court gave effect to Register.com's policy on use of its system, even though the policy did not purport to restrict access to the system itself, *Register.com* is interesting because the court presumably could have inquired whether Verio had notice of and manifested assent to Register.com's terms. It conducted precisely that inquiry in connection with Register.com's contract claim.[290] For purposes of the CFAA claim, however, the court gave effect to Register.com's terms without an inquiry into issues of notice or assent.

An equally broad, if not broader, approach to finding unauthorized access is manifested in *EF Cultural Travel BV v. Explorica, Inc.*,[291] a case involving a dispute between a tour company and one of its former employees over use of information available on EF's website. The former employee established a rival company and sought to undercut EF's prices by using a "scraper"—a program designed to extract certain publicly available information from EF's website.[292] To assist in the tool's development, the former EF employee provided a software developer with certain information about tour codes used on EF's website. Although the codes themselves were publicly available on the site, they were not readily understandable to the public.[293] Nothing in EF's terms of use prohibited use of an automated tool such as a scraper.[294] The question was whether Explorica's access to EF's site was nevertheless unauthorized for purposes of § 1030(a)(4), which prohibits one from "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value."[295] The district court concluded that the scope of authorization to use EF's website should be determined by the "reasonable expectations of both EF and its ordi-

---

[289] *Id.* at 249, 251 (noting that access to information is unauthorized because Register.com objected to it; referring back to trespass discussion, in which court concluded that filing of lawsuit signaled Register.com's objection).

[290] *Id.* at 248 ("Nor can Verio argue that it has not assented to Register.com's terms of use.").

[291] 274 F.3d 577 (1st Cir. 2001).

[292] *Id.* at 579.

[293] *Id.* at 579, 583.

[294] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003).

[295] 18 U.S.C. § 1030(a)(4) (2000).

nary users."[296] The court found several indications that Explorica's use of the scraper was inconsistent with the reasonable expectations of the parties, in light of copyright, contractual, and technical restrictions on the site.[297] On appeal, the First Circuit found it unnecessary to rule on the district court's "reasonable expectations" test because it found an alternative basis for concluding that Explorica's scraper was unauthorized under the CFAA: Its development depended on the former employee's use of proprietary information—the tour codes—in violation of a confidentiality agreement.[298] In other words, even where no policy restricted access to EF's publicly available website, a court found access to be unauthorized based solely on an external contractual agreement. That agreement, however, did not explicitly relate to use of EF's publicly available website; thus, the former EF employee did not actually assent to restrictions on use of that site. Accordingly, reading the confidentiality agreement to curtail access to the website is somewhat analogous to validating a policy statement that purports to limit uses of a system, without inquiry into issues of notice and assent.

In a separate appeal arising from the same set of facts but involving the company that actually developed the scraper, *EF Cultural Travel BV v. Zefer Corp.*,[299] the First Circuit more explicitly embraced an approach validating limits on access embodied in a policy statement. The scraper's developer urged that it had no knowledge that the scraper was based on confidential information, and that the injunction against its use of the scraper therefore could not be affirmed on the same basis as the injunction against the former EF employee.[300] The court of appeals agreed and therefore necessarily had to consider the propriety of the district court's "reasonable expectations" test. The court rejected that test,[301] concluding instead that lack of authorization for purposes of the CFAA could be established "by an explicit statement on the website restricting access."[302] Because EF had no such explicit prohibition at the time of the developer's use of the scraper, that use did not violate the CFAA.[303] The significance of this second decision lies in the court's suggestion in

296 *Explorica*, 274 F.3d at 580.

297 *Id.* at 580–81.

298 *Id.* at 581–82.

299 318 F.3d 58.

300 *Id.* at 61.

301 *Id.* at 62.

302 *Id.*

303 The court of appeals nevertheless affirmed issuance of the injunction on the theory that any use of the scraper would assist Explorica in violating the injunction against it. *Id.* at 63.

dictum that violation of policies purporting to limit access to EF's system could form the basis of an unauthorized-access claim: The court announced that "[i]f EF wants to ban scrapers, let it say so on the webpage or a link clearly marked as containing restrictions."[304] The court mentioned that public policy might displace certain terms,[305] but appeared to assume that a policy announcing permissible uses would provide sufficient notice of what conduct was prohibited to trigger liability under the CFAA.

In sum, just as courts have looked to policy statements to signal limitations on access in trespass claims, so too have courts focused on such mechanisms to conclude that defendants' conduct violates the CFAA. I depict courts' approaches to CFAA claims, along with those of courts addressing trespass and contract claims, in Figure 3 in Part III.A.4. In the bulk e-mail cases, the disputes typically involve actual notice of a plaintiff's objection to the defendant's conduct; but courts have nevertheless assumed that actions inconsistent with terms of use or general policy statements are sufficient to trigger liability. In cases seeking damages, that conclusion has been critical to courts' holdings. In cases involving recursive queries or similar tools, courts likewise focused on violations of terms in policy statements as forming the basis for unauthorized-access claims.

3. *Contract Law*

Although network resource owners wishing to block unwanted uses of their systems have relied mainly on trespass-to-chattels and CFAA claims, they have also raised contract claims on occasion. Of course, to argue that particular activities breach contractual limitations on uses of a system, the system owner must be able to make a plausible claim that a user had notice of and assented to the limitations. Contract claims typically arise in one of two contexts: when a bulk e-mailer is a subscriber of a particular service and uses that service either to transmit unwanted e-mail or to extract e-mail addresses in violation of a subscriber agreement; or when a website contains terms of use to which a web server owner claims that a user assented, either by affirmatively clicking "I Agree" where necessary or merely by using the site.

---

304 *Id.*

305 *Id.* at 62 (observing, after stating that explicit terms on website could establish lack of authorization, that "[w]hether public policy might in turn limit certain restrictions is a separate issue").

Hotmail[306] provides an example of the former type of case. The court there found that the bulk e-mailers who maintained Hotmail accounts had assented to restrictions on the sending of unsolicited commercial or pornographic e-mail.[307] Similar claims presumably could have been made in the cases involving the harvesting of e-mail addresses and transmission of bulk e-mail to AOL users, since it was acknowledged that the defendants were AOL subscribers. *Register.com*[308] and *Ticketmaster*[309] are examples of the latter "terms of use"-based rationale for contract breach. Register.com alleged that its terms of use forbade Verio from using information from its database for solicitation purposes. Verio's submission of a search query to its database, Register.com argued, constituted its acceptance of those terms of use, and Verio breached the contract so formed.[310] Similarly, in *Ticketmaster*, Ticketmaster claimed that Tickets.com, by using its site, agreed to terms that forbade the sort of automated queries in which Tickets.com engaged.[311]

Unlike trespass doctrine and the CFAA, which are silent as to what triggers a system owner's right to exclude unwanted uses, a contract claim requires the system owner to show that the user had notice of and assented to certain limitations on use of the system.[312] As with trespass and CFAA claims, however, there has been variance in the strength of the notice provided and the clarity with which assent has been manifested. To understand the situations in which courts might enforce limitations on use of a system, it is helpful to examine the controversial issues of notice and assent that have arisen from the enforcement of standard form licenses that often accompany software. For example, manufacturers often include licenses inside software boxes and seek to treat the consumer's act of breaking the shrinkwrap as assent to the governing terms.[313] The trend among courts is to enforce such "shrinkwrap" licenses, so long as the consumer has a

306 Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020, 1025 (N.D. Cal. 1998).

307 *Id.*

308 Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004).

309 Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).

310 *Register.com*, 126 F. Supp. 2d at 244, 248.

311 *Ticketmaster*, 2003 WL 21406289, at *2.

312 *See, e.g.*, Specht v. Netscape Communications Corp., 306 F.3d 17, 28–30 (2d Cir. 2002) (discussing notice and assent requirements).

313 ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996). For discussion of the contract formation and copyright preemption issues such licenses raise, see generally Lemley, *supra* note 145, and Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995).

right to reject the terms by returning the product.[314] Extending this reasoning to the online context, courts have enforced "clickwrap" or "click-through" licenses that require a user to click "I Agree" or "I Accept" before downloading a particular product, at least so long as the user has reasonable notice of the existence of the governing license terms and the "offer" makes clear that clicking the button will signify assent to those terms.[315] No court finding that these conditions have been met has declined to enforce a clickwrap agreement purporting to govern the download of a software product on grounds of insufficient assent.[316]

For purposes of this Article, the question is how the reasoning of these cases involving the purchase or download of software products

---

[314] *See, e.g.*, *ProCD*, 86 F.3d at 1452–53 (finding license included in software package binding, where license terms also appeared on user's screen every time software ran, user could not proceed without indicating acceptance, and user had opportunity to return software for refund if terms were unacceptable); Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149–50 (7th Cir. 1997) (finding list of terms contained inside computer box enforceable, when purchaser had option to return computer within 30 days of receipt if terms were unsatisfactory). A handful of cases pre-dating the *ProCD* decision had refused to enforce shrinkwrap agreements. *See* Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 105–06 (3d Cir. 1991) (refusing to enforce warranty limitations printed on outside of software package, where terms differed from those in purchase order; treating limitations on package as additional terms proposed by manufacturer and never accepted by purchaser); Ariz. Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 766 (D. Ariz. 1993) (following *Step-Saver*); *see also* Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 269–70 (5th Cir. 1988) (concluding that federal copyright law preempted provisions of state law on which shrinkwrap license relied, thus rendering license unenforceable). For decisions questioning or distinguishing *ProCD*, see *SoftMan Products Co. v. Adobe Systems, Inc.*, 171 F. Supp. 2d 1075, 1087–88 (C.D. Cal. 2001), holding that a software distributor was not bound by license terms because the reseller did not actually run the software, and thus never agreed to terms, and *Klocek v. Gateway, Inc.*, 104 F. Supp. 2d 1332, 1341 (D. Kan. 2000), refusing to enforce terms contained inside a box for a personal computer because plaintiffs did not expressly agree to the terms and were not informed of the manufacturer's policy that failure to return the computer within five days constituted agreement.

[315] *Compare* i.Lan Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002) (enforcing license where terms appeared on screen prior to software installation and defendant checked "I Agree" box), Forrest v. Verizon Communications, Inc., 805 A.2d 1007, 1010–11 (D.C. 2002) (enforcing forum selection clause where terms were displayed in scroll box and plaintiff subscriber clicked "Accept" button), Caspi v. Microsoft Network, L.L.C., 723 A.2d 528, 530–31 (N.J. Super. Ct. App. Div. 1999) (enforcing forum selection clause contained in agreement with ISP, where prospective subscriber could only access service by clicking "I Agree"), Moore v. Microsoft Corp., 741 N.Y.S.2d 91, 92 (App. Div. 2002) (dismissing claim against software manufacturer where plaintiff user clicked on "I agree" icon before downloading software and claim was barred by license agreement), *and* Barnett v. Network Solutions, Inc., 38 S.W.3d 200, 204 (Tex. App. 2001) (finding forum selection clause enforceable where plaintiff had to scroll through terms and accept them before proceeding), *with Specht*, 306 F.3d at 31–32 (finding license terms unenforceable where terms appeared only on portion of web page below software download button).

[316] Courts have recognized that specific terms may nevertheless be unenforceable. *See, e.g.*, Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1173–77 (N.D. Cal. 2002) (finding arbitration clause substantively unconscionable).

applies when the owner of a computer system purports to restrict uses of her system through terms of use. The case law suggests that, where a computer system owner sets forth the terms of use and requires the user to click a button before proceeding, the terms will be enforceable. Indeed, courts have arguably gone further than that, in allowing mere use of a system to qualify as a manifestation of assent to terms. Register.com, for example, claimed that it had an enforceable contract with Verio because a user submitting a query would see a legend restricting use of the data returned by Register.com's system.[317] The district court found Register.com likely to succeed on its breach of contract claim despite the fact that Verio was not required to click "I Agree" or "I Accept" when it encountered Register.com's terms.[318] Rather, the court found that mere use by Verio of Register.com's system constituted assent to Register.com's terms.[319] On appeal, the Second Circuit took a slightly different approach, observing that Verio had actual knowledge of Register.com's terms because it submitted so many queries.[320] On the issue of assent, the Second Circuit concluded that an explicit statement of agreement (such as clicking an "I Agree" icon) is not essential to the formation of a contract in all circumstances.[321] Similarly, in the *Ticketmaster* case, Tickets.com's spiders were not required to click "I Agree" before retrieving Ticketmaster's pages, and Tickets.com therefore argued that mere use of Ticketmaster's site could not form the basis of a contractual agreement.[322] Although the district court initially denied injunctive relief,

317 Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 396, 398–402 (2d Cir. 2004). The legend stated: "By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that under no circumstances will you use this data to . . . support the transmission of mass unsolicited, commercial advertising or solicitation via email." *Id.* at 396.

318 Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000).

319 *Id.*

320 *Register.com*, 356 F.3d at 401–02.

321 *Id.* at 403. For a discussion of the unusual posture of this case, see *supra* note 282. Judge Parker would have held that Register.com was not likely to succeed in demonstrating that a contract was formed with Verio. *Id.* at 407. Judge Parker argued that even though Verio had actual knowledge of Register.com's terms, Verio could reasonably have believed that Register.com was required to make the information in question publicly available. *See id.* at 431 (Parker, J.) ("Verio . . . may repeatedly submit WHOIS queries to Register.com based on an (accurate) understanding that Register.com does not own WHOIS information and that such information must be made freely and publicly available . . . .").

322 Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 WL 525390, at *3 (C.D. Cal. Mar. 27, 2000).

seemingly skeptical of Ticketmaster's theory,[323] it later declined to enter summary judgment against Ticketmaster on that claim.[324]

It is important not to overstate the holdings in *Register.com* and *Ticketmaster.* In both cases, the courts ultimately found that the defendant had actual notice of the terms. Because the courts found actual notice present, these particular cases do not raise some of the controversial issues of notice that arise with respect to mass-market software licenses. On the question of assent, however, the courts clearly took the view that use of a system can be deemed assent to relevant terms; the danger is that if courts accept more limited forms of notice, the result will approach a default rule of closed access.

4. *Summary*

As this discussion illustrates, across the different doctrinal contexts, courts have taken a variety of approaches to efforts to exclude unwanted uses of network resources. Figure 3 below modifies Figure 1 to summarize the legal rules accepted and rejected in the case law.

Figure 3 demonstrates that, notwithstanding the fact that the leading bulk e-mail and robot cases, *CompuServe* and *eBay*, involved actual notice of limitations on a system, a number of courts have drifted toward relying on weaker forms of notice, such as terms of use without an "I agree" requirement and policy statements posted at a given location on the network. At the opposite end of the spectrum, cases such as *Ticketmaster* and *Hamidi* explicitly reject the notion that actual notice triggers a right to enjoin an unwanted use, and implicitly reject the notion that implementation of technical mechanisms triggers a right to enjoin an unwanted use.

Having clarified the current legal landscape, I consider in the next two sections what the law should be.

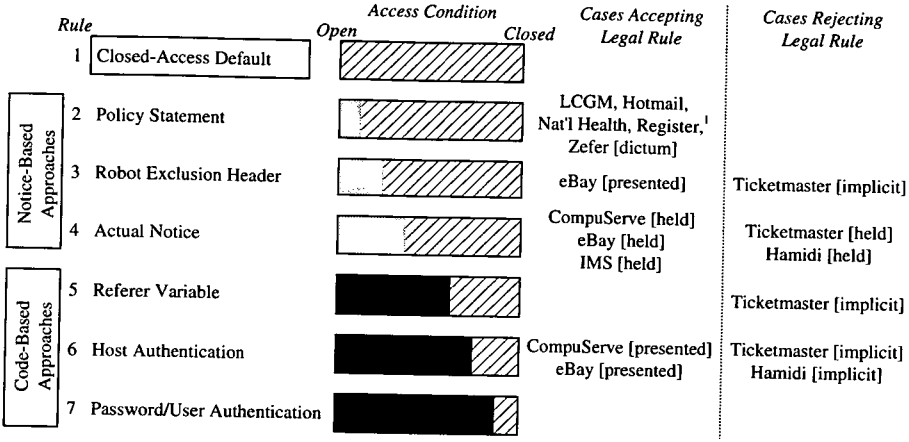
B. Curtailing the Drift Toward a Closed-Access Default

In this Section, I focus on the extent to which courts have drifted toward relying on policy statements and terms of use as setting the limits of permissible uses of the system, without adequate inquiry into notice issues. With respect to all cyberproperty claims, I will argue, this approach is doctrinally and normatively inappropriate. I thus

[323] Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 WL 1887522, at *5 (C.D. Cal. Aug. 10, 2000) ("The contract theory lacks sufficient proof of agreement by defendant to be taken seriously as a ground for preliminary injunction.").

[324] Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2003 WL 21406289, at *1–*2 (C.D. Cal. Mar. 7, 2003) (observing that "a contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases, presumptive knowledge) of the conditions accepted when doing so").

FIGURE 3
LEGAL RULES ACCEPTED AND REJECTED IN CASE LAW



[1]Policy statement approach central to holding only in *LCGM* and *Nat'l Health*, which involved damage claims for conduct that took place prior to AOL's sending of cease-and-desist letters. In all other cases plaintiffs sought injunctive relief and defendants had actual notice of objection, but courts did not rely on that actual notice.

make the case for rejecting weak forms of notice in favor of stronger ones. A necessary corollary of this analysis is that courts should never proceed from a default rule of closed access.

Decisions allowing owners of network resources to enjoin unwanted uses of their systems are controversial partly because system owners seek at the same time to grant and deny access to the same types of communications. From a technical perspective, bulk e-mail looks like ordinary e-mail; a recursive data request generated by a software program is the same as a data request generated by an individual user. As a result, those seeking to defend against unwanted access claims argue that one who connects a system to the Internet and configures it to accept or respond to certain communications thereby "consents"—implicitly, if not explicitly—to the use of the system for communications to which the system is configured to respond.

Courts have generally accepted this default rule of consent, but they have held that the system owner can limit or revoke that consent in relevant ways.[325] If we accept that a system's open configuration does provide a default rule of consent, then the question is: What must a system owner do to limit or revoke that consent in a way that will be legally effective? Even if we approach this question from a doctrinal perspective, it becomes clear that the law should require

[325] *See supra* notes 227–34 and accompanying text.

fairly strong signals of the limitations on use of a system—and that policy statements posted at some location on a network and user agreements that need not be viewed or formally "accepted" before one proceeds should not qualify.

Turning first to the trespass-to-chattels doctrine, recall that for a network resource owner to sustain a trespass claim, she must show that a particular use of a system is "unauthorized." Although scholars have resisted reliance on analogies between access to real property and access to Internet-connected network resources,[326] a real-property analogy, properly understood, is actually helpful in this context. Two rules governing trespass to real property are relevant: the general default rule for trespass, and the rule that applies once a landowner invites access. The general rule is that a property owner can recover for trespass even if she neither fences her property nor posts a "No Trespassing" sign.[327] This approach can only be justified by a theory that the would-be trespasser is in a good position to know, or to discover, that he is entering onto another's land and that the entry may be unwelcome, and thus should bear the burden of making that determination.[328] Once a landowner invites access, however, the burden shifts back to the landowner to limit or revoke the invitation. In particular, a revocation of consent is not effective until the would-be trespasser knows or has reason to know of it.[329]

---

326 *See supra* note 12.

327 *See supra* note 200 and accompanying text.

328 Indeed, scholars distinguish between circumstances in which a property rule (such as trespass) is preferable to a liability rule (such as nuisance) based on the clarity of the entitlement holder's right. For example, Professor Ian Ayres has noted:

> When Rose steals my watch or builds an encroaching wall or becomes a hold-over tenant, Rose usually knows at the time that she is unlawfully impairing my entitlement. In contrast, it is more difficult for Rose to know in advance whether her noise or dust emission will constitute a nuisance.

Ian Ayres, *Protecting Property with Puts*, 32 VAL. U. L. REV. 793, 829 (1998).

329 *See* Brabazon v. Joannes Bros. Co., 286 N.W. 21, 25–26 (Wis. 1939) (reversing judgment on trespass claim where court erroneously placed on defendant burden of showing that plaintiff consented to entry; because defendant had implied license to enter, trespass could only be found upon showing that plaintiff terminated consent); RESTATEMENT (SECOND) OF TORTS § 892A cmt. i (1979) ("[C]onsent is terminated when the actor knows or has reason to know that the other is no longer willing for him to continue the particular conduct."); RESTATEMENT (SECOND), *supra* note 24, § 171 ("Subject to the privileges of reasonable egress and removal of things, the actor's privilege to enter land created by consent of the possessor is terminated by . . . (b) a revocation of the possessor's consent, of which the actor knows or has reason to know . . . ."); *see also* Bullick v. Colebrookdale Township, No. CIV.A.96-CV-1266, 1997 WL 587248, at *3 (E.D. Pa. Sept. 12, 1997) (declining to dismiss trespass claim because factual issue remained as to whether defendant knew or had reason to know that plaintiff revoked consent to entry); Minshew v. State, 542 So. 2d 307, 311–12 (Ala. Crim. App. 1988) (holding that, for purposes of criminal trespass statute, even if defendant's initial entry had been licensed, any license to remain on premises was terminated by virtue of defendant's scuffle with homeowner); Mitchell v. Mitchell,

These real property rules show why a default presumption of closed access is inappropriate in the Internet context and why policy statements or terms of use posted at some location on a network (and not requiring explicit acknowledgment by a user) are inappropriately "weak" signals to trigger trespass-to-chattels liability. Looking to the default rule, a user moving between sites over the Internet does not experience the concept of "entry" in the same way as he would in physical space. When a system is technically configured to allow particular uses, the default presumption should be that the system owner consents to the allowed use because the system owner is in a better position to set and convey limits than a user is to discover them on his own. Moreover, if a system is technically configured to allow particular uses, whatever notice to the user the system owner provides must be strong enough to overcome that consent—to place the user in a position to know or have reason to know that consent has been revoked or limited.

Most of the cases suggesting that policy statements or terms of use posted at some location on the network are sufficient to limit or revoke consent (such as *LCGM*, *Hotmail*, *Register.com*, *National Health Care Discount*, and *Zefer*, all presented as validating Rule 2 in Figure 3) have not explicitly considered, at least with respect to the trespass to chattels and CFAA claims involved, whether such statements or terms place a user in a position to know or have reason to know of limitations on the use of the system. Courts' failure to consider such statements is surprising, since in some cases actual knowledge of the limitations was present; in *Register.com*, the court called explicit attention to this fact in connection with the contract claim.[330] As a general matter, policy statements articulating limits on use of a system that is otherwise configured to accept communications will not be sufficient to give a user knowledge of limitations on the use of the system. Taking first the example of a mail server configured to accept e-mail from any point on the Internet, one who sends e-mail to such a server would be most unlikely to know that his contacts are unwelcome (since the policy statement is only available at some location on the mail server's network).[331] Indeed, the vast majority of e-mailers

55 N.W. 1134, 1135 (Minn. 1893) (concluding that plaintiff's explicit request that defendants leave house constituted revocation of license to enter); St. Louis County v. Stone, 853 S.W.2d 437, 439 (Mo. Ct. App. 1993) (holding that, despite implied consent of owner to entry, circumstances were sufficient to place defendants on notice that they were not allowed to enter).

330 *See supra* note 320 and accompanying text.

331 Hunter, *supra* note 12, at 508–09 (describing scenario in which individual could violate "term of use" prohibiting sending of joke e-mails to university's mail server, even

are probably not even aware that their mail resides on a server, and would have no idea how to locate a mail server's open network. Similarly, if it is possible to navigate a website without encountering an indication that policies limit such access, one who so navigates a website cannot be said to know or have reason to know of the limitations. For web browsing, the strongest argument that online policy statements do constitute appropriate signals of limitations is that users *should* know that such policies exist and are on notice to inquire about the terms when they visit any site. But in light of the consent the system's code conveys, it is difficult to see policies merely posted at some location on the network as a limitation on consent. When a system owner implements some technical block, and the user must take steps to evade it, the situation is different, and revocation of consent can reasonably be inferred.

A similar result is appropriate for contract claims in this context.[332] When a policy statement is simply posted at some location on a network, without purporting to bind users to its terms, no contract claim will lie. The harder question is whether a system owner can attempt, through the language of her terms of use, to deem "use" of the site to constitute agreement to the terms and limitations.[333] This sort of approach is widespread among website owners; eBay's site provides a useful example. Although eBay requires users listing or bidding on items to register with the site, and to accept a user agreement in the process, users merely browsing the site need not do so. This fact is particularly relevant for robots extracting data from eBay's site: A robot would not encounter any technical impediment to its data extraction.[334] Despite the fact that eBay's site is open in a technical sense, the eBay home page does state that "Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy."[335] That User Agreement does not itself appear on the eBay home page; it requires a click-through to another page on the system.[336] Through this mechanism, eBay has tried to create a con-

though he would have no notice of such limitation); *see supra* note 167 and accompanying text.

332 I do not consider CFAA claims here because I argue below that the CFAA should be limited to code-based access controls. *See infra* notes 348–70 and accompanying text.

333 For discussion of cases that implicitly or explicitly adopt this approach, see *supra* notes 308–11, 317–24 and accompanying text.

334 I discuss the significance of the robot exclusion standard in greater detail below. Use of that standard does not in fact block access; it simply directs compliant robots not to query certain portions of a site. *See infra* notes 383–85 and accompanying text; *see also supra* notes 204–06 and accompanying text.

335 *See* http://www.ebay.com (last visited Aug. 21, 2004).

336 *See* User Agreement, *at* http://pages.ebay.com/help/policies/user-agreement.html (last visited Aug. 21, 2004).

tract even with those users who need not click "I Agree" in order to proceed further on eBay's site. As noted earlier, cases involving standard-form "shrinkwrap" and "clickwrap" licenses are themselves controversial in part because courts have conducted only limited inquiries into issues of notice and assent.[337] Relying on a posted statement that use of a site constitutes assent to its terms of use pushes that line of cases one step further. For that reason, at least one court declined to enforce a license associated with the download of software where users did not have to click "I Agree" to proceed.[338] To the extent that the denial of summary judgment in *Ticketmaster* and the *Register.com* district court decision suggest that mere use of a site, without more, is sufficient to bind a user to terms posted at some location on a network,[339] they are inconsistent with established rules of contract interpretation and therefore should not be followed.

Normative considerations reinforce these conclusions. To continue with the eBay example, the statement on eBay's home page that use of the site constitutes acceptance of the terms of eBay's User Agreement is a very weak form of notice of limitations on permissible uses of the site. If that notice were enough to trigger eBay's right to block unwanted uses, then eBay's ability to control its site would approach the degree of protection available in a closed-access default rule.

Quite apart from the unfairness of such a rule to users who are unlikely to have notice of the terms of use, treating such terms as the basis for trespass or breach-of-contract claims allows a system owner to achieve the benefits of closed access whenever she wishes, without internalizing any of the costs of closing access. Recall the observation in Part II that rules requiring some kind of notice to trigger a right to enjoin an unwanted use have both liability-rule and property-rule features and might usefully be described as "loperty" rules.[340] Protecting an entitlement through a "loperty" rule has two benefits. First, it eliminates the need for negotiations in cases in which a resource owner is willing to permit access. Second, it provides a mechanism to distinguish owners for whom property-rule protection is efficient from those better served by an open-access rule, by forcing a system owner

337 *See supra* notes 306–24 and accompanying text.

338 Specht v. Netscape Communications Corp., 306 F.3d 17, 32–35 (2d Cir. 2002).

339 Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2003 WL 21406289, at *2 (C.D. Cal. Mar. 7, 2003); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004). For discussion of these cases, see *supra* notes 308–11, 317–24.

340 *See supra* note 216 and accompanying text.

to assess the value of closing access and to communicate that value to would-be users.[341]

If the law requires only very weak signals to trigger property-rule protection of network resources, however, the benefits of taking a "loperty"-rule approach are lost altogether. If the signals the law requires are sufficiently weak that users are poorly situated to determine whether their use is permissible, then users must negotiate for access in all cases. (This, of course, was the basis for scholars' objection to property-rule protection for computer networks.[342]) And a regime under which only weak signals are required allows a system owner to avoid internalizing the costs of closing access.

If the law is to allow notice of permissible uses of a system to trigger legal protection for system owners, it must force stronger forms of notice than current case law appears to require. The system owner should generally bear the burden of proving that the defendant had actual notice of the objection to the challenged use. Courts could also identify other steps by a system owner that would presumptively qualify, such as employing a technical measure (even a weak one) that a user would have to defeat to gain access. eBay's configuration again provides a useful example. In order to list or bid on an item on eBay's pages, one must actually register as an eBay user. In that registration process, the user is presented with the terms of eBay's User Agreement and must click "I Agree" before completing the registration process. eBay's system is thus technically open to all users who wish merely to browse, but it is not technically open to users who wish to bid or sell. Even if we treat the initial openness of eBay as conveying consent, when it comes to bidding and selling, eBay has constructed its system to negate the consent that the code conveys—by requiring users to review and accept the user agreement before they navigate further. In this context, it is more reasonable to treat the limitation as a valid indication of the bounds of the system owner's consent to use. Even to the extent that a provider does not work on a subscription or membership model, it may configure its system so that one cannot use the network without agreeing to certain terms, by routing all traffic to a main page that requires acknowledgment of terms; there too, the fact that there are limits to the system owner's consent is conveyed to the user.[343]

---

341 *Cf.* Bell & Parchomovsky, *supra* note 101, at 53–54 (describing benefits of "fencing out" rule).

342 *See supra* notes 163–76 and accompanying text.

343 My argument that the law must require stronger forms of notice than current law seems to require, in part to force system owners to evaluate and internalize the costs of closing access, is somewhat consistent with one expounded by Michael Madison. He has

The key in each of these examples is that, once the system's code signals that there are some limits on use of the system—by forcing the user to acknowledge the existence of these limits—it is no longer reasonable for a user to assume that the system owner consents to any and all uses. Because this approach places the burden on the system owner to configure the system in order to alert users of the limitations on access, it forces the system owner to weigh the benefits of closing access against that burden and thus captures the benefits of a "loperty" rule approach.

C. The Choice Between Notice-Based, Code-Based, and Commons Approaches

In the previous Section, I argued that, for doctrinal and normative reasons, courts must at a minimum curtail the drift toward a closed-access default rule, by requiring stronger signals of the limitations on use of a system to trigger a right to enjoin unwanted uses. That still leaves open the question of which of the remaining approaches is preferable—a notice-based approach (as narrowed by the discussion above to mean actual notice or adoption of a system configuration that makes it plain to the user that use is restricted); a code-based approach; or a commons approach. Recall that both notice-based and code-based approaches can be characterized as combining liability-rule and property-rule treatment of a network resource. The difference between the two approaches is that more is required under a code-based approach to trigger the property-rule protection: The system must use a technical measure that actually controls access to some degree.

The choice between these approaches, too, has both doctrinal and normative components. I first consider the doctrinal issues. Doctrinal considerations establish that, under the CFAA, courts should recognize a legal right to exclude unwanted uses only in connection with technical measures that are effective in controlling access to a system.[344] Although a similar doctrinal argument could be made for

---

argued that courts should require a system owner wishing to enforce an access limitation to demonstrate "a salient or visible boundary between open, public information and information subject to access constraints." *See* Madison, *supra* note 12, at 491. Madison, however, would conclude that "[g]iving actual notice of the access restriction to the individual user may not be sufficient." *Id.* In addition, under Madison's view, "[a] mere 'No Trespassing' 'sign' on the Internet, such as the robots.txt file . . . is easily ignored as a triviality on the Internet as a whole." *Id.* at 498.

[344] *See infra* Part III.C.1. Two recent articles identify problems with current judicial approaches to the CFAA similar to those that I identify. *See* Galbraith, *supra* note 142, at 323–24 (arguing that, although CFAA was designed to combat computer crime, statute "is now being used to control access to and the use of information contained on publicly avail-

trespass to chattels, I conclude that it is not compelling.[345] The remaining questions are largely normative. The main normative consideration that has been overlooked thus far is that recognizing strong code-based approaches will tend to give system owners incentives to achieve through code what they cannot achieve through law alone. Analyzing cyberproperty claims in light of that consideration leads me to an approach under which an appropriate form of notice—either actual notice or use of a particular configuration that presumptively satisfies the notice requirement—triggers a system owner's right to enjoin unwanted uses.

1. *Doctrinal Issues: The Computer Fraud and Abuse Act*

As discussed earlier, plaintiffs seeking to control access to network resources typically invoke sections of the CFAA that prohibit "access" to a protected computer that is "without authorization" or that "exceed[s] authorized access."[346] The question is whether "access" to a protected computer "without authorization" or "exceed[ing] authorized access" encompasses only breaches of code-based limitations on access, or if other activities inconsistent with a system owner's policies or terms of use also qualify. Turning first to the statutory language, the critical questions are how we should interpret the term "access" and how we should define what conduct is without or in excess of "authorization."

We can posit two possible readings of the term "access." First, it is possible to adopt a broad reading, under which "access" means any interaction between two computers. In other words, "accessing" a computer simply means transmitting electronic signals to a computer that the computer processes in some way.[347] A narrower under-

able websites"); Kerr, *supra* note 202, at 1599 (arguing that "broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web"). Although we all agree that current judicial interpretations of the CFAA are problematic, our arguments differ in important respects. Professor Galbraith effectively concedes that the literal language of the CFAA "appears to include protection for any type of information," Galbraith, *supra* note 142, at 331, and thus rests her arguments on the CFAA's legislative history. In addition, Gailbraith argues for an amendment to the statute rather than an alternative judicial interpretation. *Id.* at 366–67. I argue that there is in fact a textual basis for a narrower interpretation of the CFAA. *See infra* notes 348–55 and accompanying text. Although Professor Kerr proposes an alternative judicial interpretation as well, he would rely on the "without authorization" language of the statute to supply a limiting principle, *see* Kerr, *supra* note 202, at 1646–60, whereas my approach would also find an outer boundary on the term "access." In addition, Kerr's main arguments are policy-based rather than textual. *See id.* at 1648–60 (discussing policy reasons for interpreting statutory terms in particular ways).

[345] *See infra* Part III.C.2.

[346] *See supra* notes 258–61 and accompanying text.

[347] Professor Kerr adopts this approach. *See* Kerr, *supra* note 202, at 1646–47.

standing of "access" would focus not merely on the successful exchange of electronic signals, but rather on conduct by which one is in a position to obtain privileges or information not available to the general public. The choice between these two meanings of "access" obviously affects what qualifies as unauthorized conduct. If we adopt the broader reading of access, and any successful interaction between computers qualifies, then breach of policies or contractual terms purporting to outline permissible uses of a system can constitute unauthorized access to the system. Under the narrower reading of access, however, only breach of a code-based restriction on the system would qualify.

Which interpretation is correct? Several prohibitions in the CFAA describe conduct that could only be accomplished through breach of a code-based limitation. As a result, the narrower reading of "access" is in fact the more natural one. The provisions clearly contemplate conduct that involves obtaining information not generally available to the public, including national security information and financial and other records,[348] or conduct that involves access to computers that are nonpublic.[349] Since the information is not available to the public, it is necessarily segregated by code—whether by a password or other technical measure, or by being placed on a system not generally accessible to the public. If "access[ ] without authorization" is to be read consistently throughout the statute, then it must extend only to breaches of these sorts of code-based limitations. Some provisions of the CFAA, of course, also contemplate conduct that "exceed[s] authorized access," and it is conceivable that restrictions in policy statements or terms of use should be relevant there. Because such provisions are designed to target activities by persons whose access to the system is not constrained by code in the same way as the general public's, such provisions align with a reading of "access[ ] without authorization" that depends on breach of code-based limitations on access. In fact, in applying a separate federal statute that protects electronic communications, courts have read the language "access[ ] without authorization" to require breaching code-based access limitations.[350]

---

348 *See* 18 U.S.C. § 1030(a)(1), (2)(A) (2000).

349 *See id.* § 1030(a)(3).

350 The statute, a portion of the Electronic Communications Privacy Act often referred to as the Stored Communications Act (SCA), 18 U.S.C.A. §§ 2701–2709, 2711–2712 (West 2000 & Supp. 2004) prohibits "access[ing] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ing] . . . access to a wire or electronic communication while it is in electronic storage in such system." *Id.* § 2701(a)(1). Plaintiffs in a number of courts have attempted to invoke the statute's civil liability provision to block others from retrieving information from their systems. *See, e.g.*,

In addition, a broader reading of access—as encompassing any interaction between computers—would create other statutory anomalies. In 1994, Congress added a computer damage provision to the CFAA;[351] as amended in 1996,[352] this provision prohibits one from "caus[ing] the transmission of a program, information, code, or com-

---

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879–80 (9th Cir. 2002); Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 820–21 (E.D. Mich. 2000); Educ. Testing Serv. v. Stanley H. Kaplan, Educ. Ctr., Ltd., 965 F. Supp. 731, 740 (D. Md. 1997). Because the statute covers the facilities of those who provide electronic communications services to others, *id.* § 2701(a)(1), and not the facilities of the users of those services, and because the statute defines "electronic storage" narrowly, *see* 18 U.S.C. § 2510(17) (2000 & Supp. I 2001), the statute should not be read to protect servers that merely make information available for retrieval indefinitely or computer systems that do not involve the provision of communication services. Courts have ignored these threshold requirements in several cases and have proceeded to consider other aspects of the claims. In doing so, however, courts seem to presume that the relevant limitations on authorization are those established by the system's code. In *Educational Testing Service (ETS)*, for example, the district court considered ETS's claim that Stanley Kaplan employees violated the Stored Communications Act by copying down questions they accessed through ETS's computerized GRE testing system in order to undermine public confidence in the test and to gain an advantage in developing test preparation software–uses that exceeded the authorization embodied in terms of use conveyed by ETS at the start of the test. *Educ. Testing Serv.*, 965 F. Supp. at 737, 740. The *ETS* court rejected that argument, concluding instead that the scope of authority to access a system depends on the computer system's technical restrictions, not on notice-based restrictions announced to end-users about how the information can or cannot be utilized: "[T]he wrongful acts targeted by the [SCA] are those committed while a user is in electronic 'contact' with a computer facility, not those committed after the user has signed off." *Id.* at 740.

Similarly, in *Sherman*, the court considered an SCA counterclaim based on Salton Maxim's allegation that its former product representative to K-Mart, Sherman, improperly gained access to Salton Maxim's confidential sales data on K-Mart's computer after Salton Maxim terminated him but while he was still representing other companies to K-Mart. *Sherman & Co.*, 94 F. Supp. 2d at 819. The court rejected Salton Maxim's counterclaim, holding that Sherman's access was not "without authorization" because there was no clear or explicit restriction on access to Salton Maxim's files with K-Mart, nor was that access restricted by any technical means. *Id.* at 821; *see also Konop*, 302 F.3d at 879 n.8 ("There is some indication in the legislative history that Congress intended *the configuration of the electronic communication system* to 'establish an objective standard [for] determining whether a system receives privacy protection.'" (quoting H.R. REP. No. 99-647, at 41) (emphasis added)).

Because § 2701(a) of the SCA does not apply to communications obtained "through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public," 18 U.S.C. § 2511(2)(g) (2000), it is unlikely that a website owner could invoke the SCA to block access to her site. The systems involved in the cases discussed above were not readily accessible to the general public, and none of the cases cited § 2511(2)(g). The courts' views that the SCA requires a breach of a technical limitation on access thus appear to flow from the "access[ ] . . . without authorization" language itself, not from § 2511(2)(g).

351 Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001(b), 108 Stat. 1796, 2097–98.

352 Economic Espionage Act of 1996, Pub. L. No. 104-294, sec. 201, § 1030(a)(5)(A), 110 Stat. 3488, 3492.

mand, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer."[353] In the 1996 amendment, Congress also enacted a provision prohibiting intentionally accessing a protected computer without authorization and thereby causing damage.[354] If access is so broadly conceived as to cover any transmission of electronic signals that are successfully received by a computer, then the two provisions—§ 1030(a)(5)(A)(i) and § 1030(a)(5)(A)(iii)—would become redundant because under the broad reading of access, one who "caus[es] the transmission of . . . code" to the protected computer actually "access[es]" the computer as well. It is a well-established canon of statutory interpretation that courts should not interpret provisions of a statute in a way that makes other provisions superfluous.[355]

The legislative history of the statute also supports a narrow reading. When it passed the first version of the computer crime statute in 1984,[356] Congress clearly sought to target hacking activities. The House Report accompanying the statute stressed both governments' and businesses' growing reliance on computers and the threat that increased networking would make society more vulnerable to hacking incidents.[357] As initially enacted, the statute covered a fairly narrow range of computers, none of which were available to the general public. In particular, the statute protected access to three types of computers: those containing national security information; those containing financial data; and those operated by or on behalf of the government.[358] When Congress amended the statute in 1986, it retained the three offenses of the 1984 act, while tweaking some elements, and added three new offenses.[359] Two of the new offenses were, like the offenses in the original 18 U.S.C. § 1030, unauthorized-access offenses. Both of these new offenses covered access to "Federal

---

353 18 U.S.C. § 1030(a)(5)(A)(i) (Supp. I 2001) (original version at 18 U.S.C. § 1030(a)(5)(A)). For an explanation of the shift in the numbering of the statute, see *supra* note 264.

354 Economic Espionage Act, sec. 201, § 1030(a)(5)(C), 110 Stat. at 3492. The provision now appears at 18 U.S.C. § 1030(a)(5)(A)(iii) (Supp. I 2001).

355 *See, e.g.*, Nat'l Endowment for the Arts v. Finley, 524 U.S. 569, 609 (1998) ("Statutory interpretations that 'render superfluous other provisions in the same enactment' are strongly disfavored." (citation omitted)); Ratzlaf v. United States, 510 U.S. 135, 140–41 (1994) (stating that courts should be particularly wary of finding statutory provision superfluous "when the words describe an element of a criminal offense").

356 Counterfeit Access Device and Computer Fraud and Abuse (Counterfeit Access Device) Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190.

357 *See* H.R. REP. No. 98-894, at 8–12 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694–97.

358 Counterfeit Access Device Act § 2102, 98 Stat. at 2190–91.

359 *See* CFAA, Pub. L. No. 99-474, § 2, 100 Stat. 1213, 1213–14.

interest computers,"[360] a term defined in two ways. The statute first defined the term to include computers

> exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer.[361]

This definition still tied the offenses to those computers containing sensitive confidential information. The statute also defined "Federal interest computer" as a computer "which is one of two or more computers used in committing the offense, not all of which are located in the same State."[362] This definition was far broader, in that it allowed coverage of unauthorized access merely if the offense involved an interstate element. Nothing in the debate over the statute's passage or the accompanying reports, however, indicates that Congress intended to extend the statute's coverage to publicly available information on such computers; on the contrary, the legislative record continued to stress issues of security and confidentiality.[363] These same concerns are reflected at the time of the passage of the 1996 amendments,[364] which adop-

---

360 *Id.* sec. 2(d), § 1030(a)(4)–(5), 100 Stat. at 1213–14.

361 *Id.* sec. 2(g)(4), § 1030(e)(2)(A), 100 Stat. at 1215.

362 *Id.* sec. 2(g)(4), § 1030(e)(2)(B), 100 Stat. at 1215.

363 *See, e.g.*, 132 CONG. REC. 28,821 (1986) (statement of Rep. Hughes) (noting that bill was designed to "deter[ ] the emergence of the computer criminal"); *id.* (statement of Rep. Wyden) (discussing dangers of hacking); *id.* at 27,640 (statement of Sen. Trible) (discussing need to ensure that "our criminal justice system is capable of addressing the types of offenses that have accompanied the rise of new technologies" and pointing in particular to acts of "theft, vandalism, and trespass" of computer data); *id.* at 27,639 (statement of Sen. Thurmond) (stating that legislation was designed "to address the real and growing danger of computer crime"); *id.* at 12,109 (statement of Rep. Rodino) (noting that legislation seeks to deter "future attempts by high technology criminals in our society"); *id.* at 7816 (statement of Rep. Hughes) (stating that legislation targets "the computer sophisticated criminal who combines his technological skill with old-fashioned greed and criminal intent to rob banks or destroy business records or steal trade secrets").

364 *See, e.g.*, 142 CONG. REC. 27,118 (1996) (remarks of Sen. Leahy) (stating that act will protect "privacy, security, and reliability of computer networks"); *id.* at 25,910 (statement of Rep. Goodlatte) (stating that act will provide "much needed protection for our Nation's important information infrastructure and help maintain the privacy of electronic information"); *id.* at 23,783 (statement of Sen. Kyl) (stating that act will "strengthen current public law on computer crime and protect the national information infrastructure" and "protect banks, hospitals, and other information-intensive businesses which maintain sensitive computer files from those who improperly enter into computer systems"); *id.* at 23,784 (statement of Sen. Leahy) (arguing that existing statute fell short in protecting "privacy and confidentiality of information").

ted the "protected computer" language that now appears in the statute.[365]

Other considerations support a narrow reading of the statute as well. Although the cases discussed earlier involve actions under the CFAA's civil suit provision,[366] the CFAA is a criminal statute, and interpretations of a statute in a civil context will carry over into the criminal context. The approach some courts have taken thus far—treating as unauthorized access any conduct inconsistent with policies posted at some location on a network[367]—might raise due process concerns, in that criminal liability would attach without a user having fair notice of the prohibited conduct.[368] This approach seems particularly troubling in light of the fact that the CFAA is a criminal statute: The approach used by these courts would suggest that a violation of the statute could occur in circumstances when a court would not even find a breach of contract.[369] Even in cases where a system owner uses strong signals (but without a technical control) to identify limitations on use of the system, an interpretation that tied liability to activities inconsistent with such limitations would criminalize a broad range of conduct, even an employee's use of a computer for personal activities in violation of an employer's policy.[370]

Courts would better serve both the statutory intent of the CFAA and public policy by limiting its application to unwanted uses only in connection with code-based controls on access.

2. *Doctrinal Issues: Trespass to Chattels*

Because the substantive elements of the CFAA and state-law trespass claims have been interpreted quite similarly, my conclusion that the CFAA should be read to cover only breaches of code-based access controls raises the question whether trespass-to-chattels doctrine should be limited in this manner as well. Does one "use" or "intermeddl[e] with" a system when one merely sends electronic signals that cause the system to respond in some way, or does "use" or "intermeddling" require a further showing that the defendant *evaded a technical or physical limitation* on use of a system? Although scholars have criticized many aspects of trespass-to-chattels doctrine,

---

365 Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(4)(A), 110 Stat. 3488, 3493 (codified as amended at 18 U.S.C. § 1030(e)(2) (2000 & Supp. I 2001)).

366 18 U.S.C. § 1030(g) (Supp. I 2001); *see supra* note 257 and accompanying text; *supra* Part III.A.2.

367 *See supra* notes 264–305 and accompanying text.

368 *See* Kerr, *supra* note 202, at 1659.

369 Lemley, *supra* note 12, at 528 n.29.

370 *See* Kerr, *supra* note 202, at 1632–37 (discussing use of CFAA in employee misconduct cases).

they have not addressed this precise question. As I show below, although there is an argument to be made for tying trespass to chattels to breach of a code-based limitation, the case for doing so is not as compelling as in the CFAA. I sketch the argument here but ultimately conclude that (like the issue of harm) the question cannot be resolved at the level of doctrine.

To understand the basis for arguing that trespass to chattels requires breach of a code-based limitation, recall one of the threshold conclusions in the *CompuServe* case: that electronic signals are sufficiently "tangible" to give rise to a trespass cause of action.[371] Scholars have disputed this conclusion on the ground that the case law on which *CompuServe* relied does not support the conclusion.[372] Even if one accepts the conclusion, as the *CompuServe* court did, that electronic signals are sufficiently "tangible" to support a trespass-to-chattels cause of action, it does not necessarily follow that any transmission of signals constitutes intermeddling. The *CompuServe* court simply concluded that sending electronic signals does qualify as intermeddling. One might argue that there is a missing link in this analysis: Even if transmission of electronic signals causes a recipient computer *to take some further action*, that does not automatically constitute use of or intermeddling with the system, considering that the system is simply processing electronic signals that it is designed to process. Under an alternative approach, a court might find use or intermeddling only if a defendant *evaded a technical or physical limitation* on use of a system, and thereby caused the system to process electronic signals in a way that it was *not* configured to process them. In other words, the issue is not so much whether electronic signals are sufficiently "tangible" to give rise to a trespass, but whether those electronic signals evade a technical limitation on the system.

---

371 CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); *see supra* note 26 and accompanying text.

372 In particular, Professor Burk has argued that *CompuServe* relies heavily on *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468 (Ct. App. 1996), and that *Thrifty-Tel* erroneously intermingles trespass-to-land and trespass-to-chattels cases. *See* Burk, *supra* note 14, at 32–33. A second criticism of the *Thrifty-Tel* case often attributed to Burk's article is that the court relied for tangibility on "particulate trespass" cases that in fact involved dispossession. *See id.* at 33–34. The cited cases did not in fact involve dispossession, and the implication that they did apparently arose only from an editorial error in Burk's article. *See* DAVID MCGOWAN, THE TRESPASS TROUBLE AND THE METAPHOR MUDDLE 7 n.31 (Univ. of Minn. Law Sch. Legal Studies Research Paper Series No. 04-5, 2004), *available at* http://papers.ssrn.com/sol3/papers.cfn?abstract_id=521982 (disputing that particulate trespass cases on which *Thrifty-Tel* relied involved dispossession).

One could further argue that *Thrifty-Tel, Inc. v. Bezenek*,[373] on which *CompuServe* relied to find intermeddling,[374] in fact involved a breach of such a technical limitation on Thrifty-Tel's system. In *Thrifty-Tel*, two teenage boys, the Bezenek brothers, sought to use Thrifty-Tel's system to make long-distance calls without paying for them. Thrifty-Tel's system contained two layers of code-based protection. To make phone calls, Thrifty-Tel customers had to enter both an access code and an authorization code.[375] The Bezenek boys obtained an access code from a friend; they then attempted, both manually and through the use of a modem and automated software, to guess a legitimate authorization code.[376] The California appellate court's opinion suggested that Thrifty-Tel's system was structured so as to dedicate a phone line to one who entered an access code alone, even if one did not enter a proper authorization code.[377] In other words, as the boys attempted to guess an authorization code that would allow them to make long-distance calls, they tied up Thrifty-Tel's phone lines. The court thus found that the Bezenek boys had made unauthorized use of Thrifty-Tel's "chattels"—i.e., its computer and phone system—and caused harm by depriving Thrifty-Tel of the ability to serve its legitimate customers.[378]

The *CompuServe* court simply used *Thrifty-Tel*'s trespass analysis to support the proposition that electronic signals transmitted to CompuServe's equipment were sufficiently tangible to support a trespass cause of action.[379] To the extent that *Thrifty-Tel* focused on the Bezenek boys' search for an *authorization* code, having already gained access to the Thrifty-Tel phone lines by entering the *access* code, the parallel between the boys' activities in *Thrifty-Tel* and the bulk e-mailer's activities in *CompuServe* was strong: In both cases, the alleged trespassers transmitted electronic signals to systems designed to receive them, but in unusually high volume. The *CompuServe* court, however, could just as easily have read *Thrifty-Tel* to foreclose CompuServe's claim. In particular, had the court focused on the boys' *prior* use of an *access* code to cause Thrifty-Tel's system to dedicate

---

373 54 Cal. Rptr. 2d 468 (Ct. App. 1996).

374 *CompuServe*, 962 F. Supp. at 1021 ("Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action." (citing *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473)).

375 *Thrifty-Tel*, 54 Cal. Rptr. 2d at 471.

376 *Id.*

377 *See id.* (noting that Bezenek boys' use of computer software in attempt to identify authorization codes generated over 1300 calls, "denying some subscribers access to phone lines").

378 *Id.* at 471–73.

379 *CompuServe*, 962 F. Supp. at 1021.

phone lines to their use in the first place, it might have concluded that *Thrifty-Tel* involved the boys' "entry," through the use of an access code, into a private area of Thrifty-Tel's phone system. In other words, use of the access code itself evaded a *technical* limitation on Thrifty-Tel's system. When *Thrifty-Tel* is viewed in this light, Cyber Promotions's conduct is distinguishable: Cyber Promotions simply caused CompuServe's system to process the sorts of signals that CompuServe's system was designed to process.

Even though the *Thrifty-Tel* case could have supported a different result in *CompuServe* and subsequent cases, the choice between notice-based and code-based trespass claims is not as easily resolved as a matter of doctrine as is the same choice under the CFAA. The textual arguments made under the CFAA simply do not apply, and the concept of "intermeddling" is underdeveloped in trespass-to-chattels case law. Choosing a code-based approach to trespass essentially requires identifying what constitutes a "restricted" area of a mail server or web server, and nothing in the existing case law resolves why the only relevant restrictions are those incorporated into code. I therefore turn now to a normative discussion to help resolve these issues.

3. *Normative Considerations: The Problem of Code*

Having set aside the CFAA on the ground that, as a matter of statutory interpretation, coverage of unauthorized "access" should be limited to activities that breach some technical limitation on access, we are left to consider the normative bases for choosing among different possible rules for other cyberproperty claims. It may be helpful at this point to return to Figures 1 and 2. As emphasized earlier, the normative choice is not merely between a property-rule approach and a liability-rule approach. Rather the choice is between a closed-access default, several different "loperty"-rule approaches (those labeled Rules 2–7 in Figure 1) with different triggers for injunctive relief, and "commons" approaches under which injunctive relief to control access is unavailable. In this last category, there are actually two different possibilities. One is a pure liability rule, under which a system owner could not enjoin unwanted access to a system, regardless of the notice-based or technical measures she employed. Because such a rule would still leave a system owner free to employ technical measures, the law would not guarantee open access—the system owner's choice whether or not to use technical measures to control access, and users' ability to circumvent any measures used, would determine the degree of access. The second possibility is a technology-displacing rule, which

would displace technical measures in particular circumstances, thereby preserving the desired level of open access.

Recall that the main concern among scholars who oppose application of trespass-to-chattels doctrine in the Internet context is that users would have to bargain for access in a significant number of cases, thereby precluding complex transactions and preventing socially valuable uses from occurring.[380] As should be clear, however, this concern does not arise with many of the "loperty"-rule approaches. Rather, it arises only with approaches that are nearer to a closed-access default (such as Rule 2 in Figure 1). To be sure, the critics' concern has some basis in the case law, insofar as the literal language of some opinions suggests that courts have relied on actions inconsistent with policy statements or terms of use to trigger liability under trespass, CFAA, and contract theories, without any detailed inquiry into whether users had notice of or assented to the relevant terms.[381] As I discussed in Part III.B, normative concerns about the extent to which bargaining must occur push us away from approaches closest to a closed-access default. They do not, however, provide a basis for choosing among the remaining rules.

Choosing among the remaining rules involving a right to enjoin unwanted uses (Rules 3–7 in Figure 1) is difficult because the rules are not conceptually distinct. Under each rule, a system owner's entitlement is initially subject only to liability-rule protection, in that the law does not back with injunctive relief a system owner's attempt to set the terms of access. The system owner is entitled to an injunctive remedy to back the conditions of access only if she satisfies a specified condition. Each rule thus reflects features of liability-rule and property-rule protection. What distinguishes the rules is that each rule demands a different, and perhaps increasingly costly, mechanism to trigger property-rule protection. In that sense, each rule presents for system owners a different cost-benefit calculus: They must measure the benefits of controlling access against the costs of maintaining that configuration, as well as the costs that the configuration will generate in blocking beneficial access, and make a decision.

It is again useful to examine eBay's approach because it illustrates some of the dilemmas system owners face. Recall that, at a technical level, eBay's site is initially open to browsing. eBay does, however, attempt to restrict the activities even of unregistered users, by deeming use of its site to constitute acceptance of eBay's user

380 *See supra* notes 163–76 and accompanying text.

381 *See supra* notes 239–46, 264–305, 316–24 and accompanying text.

agreement.[382] The relevant terms of use include a paragraph addressing "Access and Interference," which, among other things, prohibits the use of robots on eBay's site without eBay's express written permission.[383]

In light of eBay's dispute with Bidder's Edge and this term in its user agreement, one might expect eBay to use the robot exclusion standard to curtail recursive queries with entries in its robots.txt file. Yet eBay's robots.txt file directs robots to avoid only three directories on eBay's servers.[384] The robots.txt file does contain a comment stating that use of robots or other automated means to access eBay's site is prohibited,[385] but that comment is not readable by a robot. In other words, nothing in the robots.txt file directs robots to do anything but avoid a small handful of directories.

Why would eBay purport to prohibit robotic activity on its site but nevertheless allow virtually all robotic activity? We can assume that eBay has made a judgment that some robotic activity will in fact benefit the site, and that it is better off allowing all such activity to proceed, and then detecting and curtailing that which it does not

---

382 The eBay home page contains the following language at the bottom: "Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy." http://www.ebay.com (last visited Aug. 21, 2004). The opening paragraph of the User Agreement states: "If you do not agree to be bound by the terms and conditions of this Agreement, do not use or access our services." User Agreement ¶ 1, *at* http://pages.ebay.com/help/policies/user-agreement.html (last visited Aug. 21, 2004).

383 User Agreement ¶ 7, *at* http://pages.ebay.com/help/policies/user-agreement.html (last visited Aug. 21, 2004) ("You agree that you will not use any robot, spider, scraper or other automated means to access the Site for any purpose without our express written permission.").

384 The machine-readable text of the file is as follows:

> User-agent: *
> Disallow: /help/confidence/
> Disallow: /help/policies/
> Disallow: /disney/

See http://www.ebay.com/robots.txt (last visited Aug. 21, 2004). The file simply instructs all user agents (designated by the asterisk following the "User-agent" header) not to access files in three subdirectories: /help/confidence/, /help/policies/, and /disney/. eBay obviously has multiple servers, but the robots.txt files for these servers appear to be identical. *See, e.g.*, http://keyword.ebay.com/robots.txt (last visited Aug. 21, 2004); http://pages.ebay.com/robots.txt (last visited Aug. 21, 2004); http://search.ebay.com/robots.txt (last visited Aug. 21, 2004).

385 The comment states:

> The use of robots or other automated means to access the eBay site without the express permission of eBay is strictly prohibited. Notwithstanding the foregoing, eBay may permit automated access to access certain eBay pages but [solely] for the limited purpose of including content in publicly available search engines. Any other use of robots or failure to obey the robots exclusion standards set forth at <http://www.robotstxt.org/ wc/ exclusion.html> is strictly prohibited.

http://www.ebay.com/robots.txt (last visited Aug. 21, 2004).

believe will be beneficial, rather than using robot exclusion headers to deflect all such activity.[386] Because the prohibition in the robots.txt file is not machine-readable, it is too weak a signaling mechanism to trigger eBay's right to exclude. Similarly, under the approach outlined in Part III.B, the prohibition on robotic activity in eBay's user agreement—an agreement that a user of the site is required to accept only if she wishes to bid on items—would not provide eBay with the basis to control access to its site. It is not the case, then, that those wishing to index eBay's site must obtain eBay's permission; in the absence of a technical impediment or a machine-readable instruction in eBay's robots.txt file, such access should be allowed to proceed. That approach, of course, places the burden on eBay to detect unwanted activity and take steps to block it, either technically or through legal measures.

What drives a system owner's choice among the various "loperty" rules, then, is that each rule forces a system owner to make a different calculation about the costs and benefits of adopting the measure necessary to trigger property-rule protection. Here we arrive at one possible argument for preferring approaches in which property-rule protection is triggered only by actions that actually block most access to a particular resource—that is, for preferring "strong" code-based approaches. As discussed previously, one concern among scholars was that system owners would undervalue the benefits of maintaining a large-scale network.[387] Put another way, because the value of the Internet increases with its size, there will be positive externalities that system owners cannot capture through bargaining; they will therefore have too little incentive to bargain.[388] Thus, one argument for preferring a code-based approach to a notice-based approach is that such an approach would offset the unaccounted-for benefits of open access by making it more costly for a system owner to achieve property-rule protection.

It quickly becomes apparent, however, that this conception of a system owner's cost-benefit calculus is incomplete. Part II raised the possibility that a system owner can achieve the desired degree of control over her system through a combination of legal and technical measures. A system owner that perceives legal protection to be too weak is free to employ additional technical measures. In other words,

386 If the *Bidder's Edge* outcome is instructive of the way future courts will treat unwanted uses of eBay's system, eBay will only need to send a cease-and-desist letter (and possibly not even that). If the use continues, eBay can bring suit to enjoin the unwanted activity.

387 *See supra* notes 170–76 and accompanying text.

388 McGowan, *supra* note 14, at 380 & n.208.

the choice of a legal rule can prompt greater or lesser reliance on technical measures. If this is so, then we cannot prefer a code-based approach to a notice-based one simply on the theory that a code-based approach makes it more costly for a system owner to achieve property-rule protection, and thus less likely that she will do so. Assume that the law backs only very strong technical mechanisms—an approach consistent with Rule 7 in Figure 1. A system owner may still be able to choose weaker, but less costly, technical measures. Even if the law does not back these measures by prohibiting their circumvention, the measures will mimic property-rule protection to some degree.

Two questions follow. First, will system owners in fact seek to mimic property-rule protection with technical measures? I have thus far stated the concern as a theoretical one. If system owners are in fact unlikely to use technical measures when legal protection is unavailable, then those who favor requiring strong technical measures to trigger injunctive relief—or, for that matter, those who favor a pure liability-rule approach—may have the better argument, for such rules would lead to a greater degree of open access than approaches under which appropriate forms of notice or weak technical controls are sufficient to support injunctive relief. Second, even if system owners *would* pursue technical measures, might a strong code-based approach or a pure liability approach still be as good as or preferable to a notice-based or weak code-based approach? If indeed different legal rules will be combined with technical measures to yield the same degree of control for the system owner, then perhaps the choice among approaches does not matter. Alternatively, a strong code-based or pure liability approach might be preferable because the possibility of circumvention still exists—under the code-based approach, for any technical measures short of the strong measures backed by law; and under the pure liability approach, for any technical measures at all. I address these issues in turn.

Turning first to whether system owners will in fact seek to fill legal gaps with technical measures, the available evidence suggests that they will. Those system owners who are content with open access (at least in the absence of harm) are, of course, unlikely to pursue any remedy at all, legal or technical. So we need only consider those system owners for whom fully open access is not an acceptable alternative. In the major trespass cases discussed throughout this Article—*CompuServe*, *eBay*, *Ticketmaster*, and *Hamidi*—the system owner used technical measures in an attempt to block unwanted activ-

ities, before ever seeking legal relief.[389] In each of the cases, of course, the measures in question were not wholly effective, which is why the legal disputes followed. A denial of legal relief simply would have left the system owners and the would-be users to pursue ever-escalating blocking and evasion techniques. At some point, the system owners might have decided that their blocking efforts were too costly. Of course, the would-be users might just as easily have decided that the evasion techniques were too costly. Moreover, as I discuss below, the blocking measures and evasion countermeasures might impose costs on entities other than the system owners and would-be users.[390]

If I am correct that system owners are likely to employ technical measures to mimic property-rule protection, the question becomes whether this should influence our choice among legal rules. One might argue that a strong code-based or pure liability-rule approach is still preferable to notice-based or weak code-based approaches because the pure liability-rule and strong code-based approaches still allow users to evade technical measures—under a pure liability-rule approach, any technical measure; and under a strong code-based approach, any technical measure short of the strong measures backed by law. Or one might conclude that the choice among legal rules does not matter.

If we choose an approach under which actual notice (or a technical configuration making restrictions clear to the user) can trigger property-rule protection, then the system owner who uses such a mechanism will achieve control through operation of law. This is the case, of course, because once actual notice has been given, unwarranted access may be enjoined; technical measures will not be necessary. If we choose an approach under which only technical measures trigger property-rule protection, then the system owner will achieve control through operation of the technical measure, in combination with the operation of law. If we choose a pure liability-rule approach, then the system owner will achieve control through operation of the technical measure alone.

Setting up a simple choice between these approaches, however, presumes that the *balance* between legal and technical measures in producing particular levels of access does not matter. That may not be the case. In other contexts, scholars have offered a number of reasons why technical measures are dangerous regulatory tools. Although much of this literature focuses on how the availability of technical

389 *See supra* notes 95–96, 233 and accompanying text.

390 *See infra* note 406 and accompanying text.

measures adds to the government's regulatory toolbox, I argue that the concerns the literature reflects should make us wary of choosing legal approaches that are likely to induce greater reliance on technical measures to achieve protection of network resources.

The observation that technical measures can produce regulatory effects similar to laws is typically made in the context of debates over the feasibility and legitimacy of government efforts to regulate Internet-related activities.[391] In response to claims that the Internet would largely resist state regulation, for example, Professor James Boyle has argued that the state can achieve its regulatory objectives through technology—by requiring private parties to hardwire certain governmental policy choices into technology;[392] by enforcing private choices embedded in technology;[393] or merely by influencing the development of technology in such a way as to facilitate a desired policy outcome.[394] The government, as Boyle put it, "is working very hard to design its commands into the very technologies that, collectively, are supposed to spell its demise."[395] Even without the active involvement of the state in its development, the architecture of the Internet—its "code"—constrains behavior. Professor Lawrence Lessig offers the example of the code that defined one's experience as a member of America Online in 1998: One could not enter AOL's "space" without a password; one could assume any one of five identities while in that space; one could disguise one's identity with respect to other users, but not with respect to AOL; and one could "gather"

391 Three of the leading works in this field are LESSIG, *supra* note 134; James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997); and Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

392 *See* Boyle, *supra* note 391, at 202–04 (describing requirement to incorporate V-chip into television sets and requirement that digital audio tape players incorporate serial copy protection).

393 The key example is the Digital Millennium Copyright Act, which prohibits circumvention of technical measures designed to control access to copyrighted works and prohibits trafficking in technologies designed to circumvent access controls or copy protections. *See* 17 U.S.C. § 1201(a)(1)(A) (2000) (circumvention of technical measures controlling access); *id.* § 1201(a)(2) (trafficking in technology designed to circumvent access controls); *id.* § 1201(b)(1) (trafficking in technology designed to circumvent copy controls).

394 Boyle offers the example of the development of the Platform for Internet Content Selection (PICS), a technological specification that supports the labeling and filtering of Internet content. *See* Boyle, *supra* note 391, at 191–95. The government influence in this instance, however, was indirect, in the sense that PICS was partly a response to perceived overreaching by the government in regulating sexually explicit speech directly.

395 *Id.* at 204.

with others in AOL's chat rooms, but only twenty-three users would be allowed to do so at a time.[396]

Although some scholars have suggested that regulation through code offers far greater flexibility than regulation through law alone, and that the government therefore should use technology as a regulatory tool so as to preserve certain public-order values,[397] others have cautioned that code can pose significant dangers. Architecture can shape and constrain behavior over the Internet,[398] just as it does in "real space." Scholars have argued, however, that computer code is a more powerful regulatory force than other forms of architecture.[399] Though invisible to most users, the architecture of the Internet is uniquely pervasive, in that the Internet is defined entirely by code—by hardware and software elements, by the communications protocols that allow these elements to communicate with one another, and by the applications running at the endpoints. The pervasiveness of code has led to two overlapping sets of concerns among scholars.[400]

One set of concerns relates to the *process* by which code—with its profound regulatory effects—is developed. First, the fact that code is often privately developed tends to obscure the influence of the government. While one might assume that decisions about the development of code are neutral, technical decisions, in fact the government influences the development or selection of particular technologies. In some cases, as when the government mandates technical standards,[401] the involvement of the government is clear. In other cases, however, the state may shape technology indirectly, and the assumption that technology reflects neutral, private choices is mistaken.[402] In still

---

396 LESSIG, *supra* note 134, at 66–71.

397 *See* Reidenberg, *supra* note 391, at 593.

398 *Cf.* Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039 (2002) (explaining how architectural decisions can impact crime, and advocating greater government involvement in architecture).

399 This is a major theme in Professor Larry Lessig's work. *See* LESSIG, *supra* note 134. For earlier works on this same theme, see generally Lawrence Lessig, *Constitution and Code*, 27 CUMB. L. REV. 1 (1997); Lawrence Lessig, *Intellectual Property and Code*, 11 ST. JOHN'S J. LEGAL COMMENT. 635 (1996); Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759 (1999); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996).

400 I leave aside here a third significant thread in the scholarship that argues that code is problematic simply because it expands the government's regulatory power. This line of argument proceeds from the premise that less government regulation is better than more government regulation, and thus requires acceptance of a particular view of the appropriate scope of government regulation that is not specific to the Internet context.

401 *See supra* note 392 and accompanying text.

402 *See* Boyle, *supra* note 391, at 205 (discussing how regulation through code blurs lines of accountability).

other cases, private parties may embed certain substantive choices into the technology, and enforcement of those choices yields the same outcome as if these substantive choices had been made through adoption of legal rules. As Boyle argues, "the attraction of technical solutions is that they apparently elide the question of power—both public *and* private—in the first place. The technology appears to be 'just the way things are'; its origins are concealed, . . . and its effects are obscured because it is hard to imagine the alternative."[403] In other words, the appearance of neutrality obscures the lines of accountability. If one concern about the development of code is that the influence of the government is obscured, another concern is that the choice among different possible codes is so significant that the government must have some involvement in that choice. As Professor Lessig argues, "Choices among values, choices about regulation, about control, choices about the definition of spaces of freedom—all this is the stuff of politics."[404]

Even if we set aside concerns about how code is developed, we are still left with a second set of concerns about the *operation* of the code that is generated. This concern is best illustrated through scholars' comparison of code and law as regulatory mechanisms. First, because code is self-enforcing, it lacks the law's capacity to accommodate the public interest and moderate potentially unfair results. Lessig illustrates this point in comparing a contract that purports to limit one's ability to make a fair use of a copyrighted work with a technical mechanism that has the same effect:

> If a term of a contract is inconsistent with a value of copyright law, you can refuse to obey it and let the other side get a court to enforce it. The ultimate power of a contract is a decision by a court—to enforce the contract or not. . . . The same is not true of code. . . . [W]here do we challenge the code? When the software protects in a particular way without relying in the end on the state, where can we challenge the nature of the protection? Where can we demand balance when the code takes it away?[405]

In other words, because code is self-enforcing, no institution will be called upon to evaluate the choices embedded in the architecture. Even if the choices embedded in the architecture are appropriate ones, their application in particular circumstances may be inappro-

---

403 *Id.*

404 LESSIG, *supra* note 134, at 59.

405 *Id.* at 136. Lessig perhaps overstates the point because legislatures can provide balance by regulating technology directly. Indeed, regulation to displace certain technical measures, which I identify as a possible legal approach to cyberproperty claims, *see supra* pp. 2217–18, is one type of direct regulation of technology.

priate. For example, a technical measure designed to block access that a system owner perceives to be economically harmful may unintentionally block more access than the system owner intends.[406] The absence of a legal enforcement mechanism, however, means that there is no process in which overexpansive use of a technical measure can be challenged.

The fact that code is self-enforcing raises a second point. Once the code is in place, enforcement is marginally costless. Outside of the Internet context, the costs of enforcing particular legal rights may be sufficiently high that an entitlement holder will forgo enforcement. Copyright again provides a useful example. Many scholars have argued that the fact that a copyright holder cannot identify and pursue all infringers has provided "space" for uses to occur that do not undermine the value of the holder's copyright.[407] To the extent that code facilitates costless enforcement of a right, however, it allows an individual to protect an entitlement without any calculation of the marginal costs and benefits of pursuing legal action in particular circumstances.

The copyright example identifies one more concern about the nature of code in relation to law. Consider again the fact that protection of copyright through law alone will lead to some infringing uses; to the extent that those uses do not undermine the value of the author's copyright, they may in fact be socially desirable. If a copyright holder uses some technical measure to block such uses, some users will still be able to circumvent the blocking. Leaving aside application of the Digital Millennium Copyright Act (which presumably would prohibit circumvention in this context),[408] note how even if the technical mechanism is not perfectly effective, it limits those who can engage in the contested activity to a technically savvy elite. Put another way, the nature of software is such that the impact of technical controls will be quite uneven, even when their evasion is legally permissible. As technical measures become stronger, the unevenness of their effects is likely to be magnified.

These concerns shed some light on why the choice among rules for legal protection of network resources matters. The choice of a pure liability rule, or of a rule under which only strong technical measures trigger property-rule protection, might in theory result in the same level of access as other legal rules involving a different mix of legal and technical protection. But the nature of code raises concerns

---

406 For a discussion of Ticketmaster's problems in this regard, see *supra* note 96.

407 *See, e.g.*, Yochai Benkler, *Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1243 (2000).

408 *See supra* notes 7, 135–36 and accompanying text.

that a simple focus on the sum of legal and technical protection does not take into account. In particular, we must be wary of choosing legal rules that are likely to prompt too much reliance on exclusionary technical measures. Of course, my earlier doctrinal discussion of the CFAA suggests that that statute does in fact strike a balance that heavily favors technical measures as a predicate for legal protection. But for the remaining cyberproperty claims, the picture is more complicated.

As discussed above, a pure liability rule, or a rule under which only strong technical measures trigger a right to exclude, will not lead to greater open access than notice-based or weak code-based approaches. Recall scholars' concerns that recognizing a right to exclude will lead to "overpropertization" of the Internet, by forcing would-be users, under the threat of legal penalty, to negotiate for access in a wide range of circumstances. I dismissed the most extreme forms of this argument on the ground that they wrongfully equated property-rule protection with a default presumption of closed access. Even if the overpropertization problem remains, however, it is also a problem under the pure liability-rule and strong code-based approaches because the very same uses that scholars fear will be blocked by legal measures can be blocked by technical measures. Those technical measures lack the flexibility the legal process provides and progressively narrow the range of users who can gain access to network resources. The advantages that liability-rule and strong code-based approaches offer over approaches allowing injunctive relief in a broader range of circumstances, in sum, are illusory. A baseline under which actual notice of permissible uses or weak code-based mechanisms are sufficient to trigger property-rule protection is far more appropriate than scholars have thus far recognized.

Even if recognizing a system owner's right to exclude unwanted uses in this broader range of circumstances provides the correct baseline, however, it does not follow that injunctive relief will be appropriate in every situation where the triggering conditions for property-rule protection are present. If, for example, it is possible to identify a range of cases in which the prevailing motivation for denying access is anticompetitive, property-rule protection may be inappropriate. Here again, though, pure liability-rule or strong code-based approaches are not the answer, for they will still permit technical measures to prevail (albeit with different opportunities for circumvention). To ensure access in situations of anticompetitive behavior, the law would have to displace technical measures, through the approach represented as Rule 8a in Figure 2. In other words, what is required is a legal approach that not only denies a system owner's legal right to enjoin

unwanted uses, but that also dictates the scope of the technical measures the system owner is entitled to employ. Such an approach is the conceptual equivalent of the sort of copyright preemption analysis scholars advocate,[409] except that what is being displaced is not a state law doctrine that threatens a preferred balance of rights but technical measures that threaten that balance. Debates over cyberproperty claims have for the most part not considered the role of law in displacing technical measures.[410]

In sum, an approach recognizing a system owner's right to set the conditions of access, so long as she provides adequate notice of those conditions (through actual notice or adopting a system configuration that makes restrictions plain to the user), provides a better baseline for access to network resources than a pure liability rule or one requiring strong technical measures to trigger injunctive relief. In addition, where necessary to compensate for the inadequacies of this sort of property-rule protection, we must look to technology-displacing rules rather than pure liability or strong code-based approaches to achieve the appropriate level of access.

CONCLUSION

This Article has attempted to offer a more complete framework for analyzing network resource owners' attempts to block unwanted uses of their systems. The law governing cyberproperty claims remains multi-dimensional and very much in flux. It remains to be seen how the California Supreme Court's approach to electronic trespass disputes in *Intel Corp. v. Hamidi* will apply in other functional and doctrinal contexts. Although the weight of scholarship favors the *Hamidi* approach, I have argued here that property-rule protection for network resources is more appropriate than scholars have thus far recognized. A default rule of closed access is not an inevitable feature of property-rule protection; to the extent that concerns about the range of circumstances in which users must bargain for access drive opposition to property-rule protection, those concerns are adequately

409 *See supra* notes 148–49 and accompanying text.

410 In the context of debates over the anticircumvention provisions of the Digital Millennium Copyright Act, scholars have proposed legal responses rejecting property-rule protection, including: revising the DMCA, *see* Samuelson, *supra* note 136, at 543–46; adopting a "misuse" doctrine barring copyright holders from invoking the DMCA in certain circumstances, *see* Burk, *supra* note 132, at 1132–40; or recognizing users' rights to circumvent in some circumstances, *see* Cohen, *supra* note 144, at 1141–42 & n.200; Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161, 177–78 (1997). None of these proposals entails legal displacement of the underlying technical measures.

addressed through hybrid liability/property rules, under which system owners must take certain steps to trigger property-rule protection.

More fundamentally, the literature has thus far neglected the complex relationship between law and technical measures in this context—in particular, the possibility that too-weak legal protection will induce greater reliance on too-strong technical measures, whether or not the law in fact backs those measures. This observation calls into question the apparent assumption of scholars that pure liability-rule approaches or strong code-based approaches to network resources will produce open access, and it calls for further attention to how features of computer code affect the choice of an appropriate legal approach for controlling access to computer systems.

Pure liability-rule and strong code-based approaches are likely to lead to the use of technical measures that mimic property-rule protection. Because technical measures lack the flexibility of legal measures, allow costless enforcement, and have uneven effects even where circumvention is permitted, pure liability-rule and strong code-based approaches do not supply as promising an alternative to stronger legal protection as scholars suggest. To achieve an appropriate balance among the competing interests at stake in cyberproperty claims, we should look to a rule that demands adequate notice of the conditions of access and backs those conditions with property-rule protection, but is limited where necessary by technology-displacing rules.