Tulsa Law Review

Volume 44
Issue 4 *The Scholarship of Richard A. Epstein*

Summer 2009

Trespass Torts and Self-Help for an Electronic Age

Catherine M. Sharkey

TRESPASS TORTS AND SELF-HELP FOR AN ELECTRONIC AGE

Catherine M. Sharkey*

* Professor of Law, New York University School of Law. I benefited from comments received when I presented this paper at the Epstein Symposium at Tulsa Law School, at the Law and Economics Workshop at Tel Aviv University, and at a meeting of the NYC Torts Theory Group. I am grateful to Avihay Dorfman, Mark Geistfeld, Greg Keating, Ariel Porat, Peter Schuck, Ben Zipursky, and last but certainly not least, Richard Epstein, for productive engagement. The D'Agostino/Greenberg Fund provided generous summer research support and Melissa Berger served as a diligent research assistant. This topic captivated my interest several years ago; at that time, while I was a professor at Columbia Law School, Jason McInnes, Scott Rader, Anthony Rickey, and Thomas Rosen provided helpful research assistance.

INTRODUCTION: TRESPASS TO CHATTELS ON THE INTERNET

Liability for trespass to chattels (or personal property) ensnares one who intentionally takes or intermeddles with chattel in the possession of another.[1] Dubbed the "little brother of conversion" by William Prosser,[2] this tort survived in the narrow context of minor inconvenience where conversion was not an option.[3] The past decade or so has witnessed the re-emergence of the tort in a new guise, as a sword against electronic intrusions over the Internet. This nearly-forgotten tort has experienced a second life, combating myriad intrusions on the Internet, from spam and robot cases to hacking and spyware.[4] Application of this arcane common law tort to the Internet is one of the most significant recent developments in tort law.

Intel Corp. v. Hamidi[5]—an "instant legal classic" in Richard Epstein's estimation[6]—became a flashpoint of interest in cybertrespass. In that case, Ken Hamidi, a disaffected former Intel employee, set up a website, FACE Intel ("Future and Current Employees of Intel"),[7] to disparage the company and its working conditions. Hamidi sent mass emails to current Intel employees directing them to the website and attempting to enlist their support in Hamidi's cause.[8] Intel asked Hamidi to stop; when his mass emails continued, Intel attempted to block them to no avail.[9] Intel then sued Hamidi for trespass to chattels, seeking an injunction against his continued email intrusions.[10] Intel prevailed in the lower state courts, but was dealt a blow by the California Supreme Court.[11] Intel's inability to demonstrate actual damages, in terms of impairment of its server system, was found to be dispositive.[12]

Trespass to chattels is distinct from trespass to land in that it requires proof of

1. Section 217 of the *Restatement (Second) of Torts* reads: "A trespass to chattel may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another." *Restatement (Second) of Torts* § 217 (1965).

2. W. Page Keeton et. al., *Prosser and Keeton on the Law of Torts* § 14, 86 (W. Page Keeton ed., 5th ed., West Publg. Co. 1984).

3. Prosser provides a succinct account of the history of the tort. Trespass to chattels first applied to cases where the chattel was carried off (trespass *de bonis asportatis*); next it was applied to cases where goods were damaged but not taken; finally, it was applied to "any direct and immediate intentional interference with a chattel in the possession of another." *Id.* at § 14, 85. Over time, the torts of trover and conversion seemed to replace trespass to chattels.

4. Mark Gergen proposed a new tort of electronic intrusion in the (now defunct) *Restatement (Third) of Torts: Economic Torts and Related Wrongs*. *See* Am. Law Inst., *Current Projects: Restatement Third, Torts: Economic Torts and Related Wrongs*, http://www.ali.org/index.cfm?fuseaction=projects.proj_ip&projectid=15 (last accessed Oct. 19, 2009). *See also* Mark Gergen, *Electronic Intrusions in Tort Law* (unpublished ms., Sept. 14, 2004) (on file with the University of Texas School of Law).

5. 71 P.3d 296 (Cal. 2003).

6. Richard A. Epstein, Intel v. Hamidi*: The Role of Self-Help in Cyberspace?* 1 J.L. Econ. & Policy. 147, 148 (2005).

7. FACE Intel, http://www.faceintel.com (last accessed Oct. 19, 2009).

8. *Intel Corp.*, 71 P.3d at 301.

9. *Id.*

10. *Id.*

11. *Id.* at 301–02, 325.

12. *Id.* at 308 ("These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.").

actual damage—a doctrinal requirement ensconced in the *Restatement (Second) of Torts*.[13] The theoretical underpinnings of this categorical distinction require some analysis. Why should it be that those whose land has been invaded need not prove actual damage, whereas those who have suffered similar wrongdoing to their personal property must face this additional hurdle? It is not—as is often assumed—explained by a hierarchy of land interests over those of personal property. The *Restatement (Second) of Torts* speaks, after all, of the "inviolability" of one's interest in personal property.[14] Instead, what emerges as the distinguishing feature for the protection of personal property is one's "privilege to use reasonable force to protect his possession against even harmless interference."[15] *Self-help* therefore emerges as key to the demand of invocation of legal process to protect property interests against "harmless intermeddlings."[16] Given the ability to solve such problems without recourse to the law, it makes sense to impose an additional hurdle (proof of damages) on those wishing to invoke legal processes. Self-help is an adequate remedy for protection against "harmless" intermeddlings with personal property, but not in the case of land.

Given the pivotal role of self-help, it is surprising how little attention has been paid to defining its contours and providing theoretical justification.[17] The *Restatement (Second) of Torts* offers scant guidance. It provides a single example of the trespass to chattels harm requirement, that of a child climbing onto the back of a dog and pulling its ears, doing it no harm.[18] Richard Epstein has provocatively asked "whether the hoary rules of trespass to chattels should apply to [cybertrespass] in light of the functional differences between a dog's ear and the Internet."[19]

---

13. *Compare Restatement (Second) of Torts* § 158 (liability for trespass to land extends "irrespective of whether [the trespasser] thereby causes harm to any legally protected interest of the other") *and* Keeton et al., *supra* n. 2, at § 13, 75, *with Restatement (Second) of Torts* § 218 (one is liable for trespass to chattels "if, but only if" he either dispossesses the owner of the chattel, *impairs the chattel's "condition, quality, or value,"* deprives the owner of its use for a "substantial time," or causes harm to the possessor or his "legally protected interest" (emphasis added)) *and* Keeton et al., *supra* n. 2, at § 14, 85. For this reason, nominal damages are available in trespass to land cases, see e.g. *Jacque v. Steenberg Homes, Inc.*, 563 N.W.2d 154, 160 (Wis. 1997) ("[I]n the case of intentional trespass to land, the nominal damage award represents the recognition that, although immeasurable in mere dollars, actual harm has occurred."), but not in trespass to chattels cases.

14. *Restatement (Second) of Torts* § 218 cmt. e ("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.") (emphasis added).

15. *Id.* (Sufficient legal protection . . . of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.").

16. *Id.*

17. Richard Epstein's work is the notable exception. *See e.g.* Richard A. Epstein, *The Theory and Practice of Self-Help*, 1 J.L. Econ. & Policy 1 (2005). Self-help often plays an important role in limiting the reach of legal intervention. Jane Stapleton, for example, has argued that, at least in relation to claims in tort relating to pure economic loss, the common law does not assist a plaintiff who could have helped himself—for example, by contracting with the defendant. *See* Jane Stapleton, *Duty of Care: Peripheral Parties and Alternative Opportunities for Deterrence*, 111 Law Q. Rev. 301 (1995); Jane Stapleton, *Comparative Economic Loss: Lessons from Case-Law-Focused "Middle Theory"*, 50 UCLA L. Rev. 531 (2002).

18. *Restatement (Second) of Torts* § 218 cmt. e, illus. 2 ("A, a child, climbs upon the back of B's large dog and pulls its ears. No harm is done to the dog, or to any other legally protected interest of B. A is not liable to B.").

19. Epstein, *supra* n. 6, at 159.

I. SELF-HELP: THE MISSING THIRD REMEDY

The significance of the self-help remedy in trespass to chattels sheds light on an inherent limitation of the classic Calabresi-Melamed framework of entitlements protected by legal rules.[20] At its core, the Calabresi-Melamed insight reduced problems in tort (and property) law to two steps: identification of the entitlement holder, followed by determination of the level of protection: property rule (or injunction) versus liability rule (or damages).[21] *Intel v. Hamidi* provides an apt illustration of the ways in which self-help complicates the traditional Calabresi-Melamed framework which recognizes damages and injunctive relief as remedial options. Self-help is the "missing" third remedy that should be added to the Calabresi-Melamed framework.

Ken Hamidi, a disaffected employee of Intel, sent mass emails to Intel employees and continued to do so after Intel asked him to stop. Intel sued Hamidi for trespass to chattels and sought an injunction only (i.e., no money damages). The California Supreme Court rejected the claim on the grounds that (i) Intel could not demonstrate actual damages, in terms of impairment of its mail server; and (ii) injunctive relief is unavailable where money damages are available. So far, this might appear to be a typical "Rule 3" case (as defined in the Calabresi-Melamed two-by-two matrix[22]), corresponding, for example, to denial of a plaintiff's suit for an injunction to protect an entitlement to clean air against a polluter. But, it is certainly not the case that Hamidi (analogous to the putative "polluter") has an entitlement—let alone one backed by the force of law—to send his mass emails through Intel's mail server.[23] Instead, as the

20. Guido Calabresi & Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv. L. Rev. 1089 (1972).

21. The traditional justification for property-rule protection is low transactions costs; the argument is that when transactions costs are low, bargaining will lead to an efficient outcome. *Id.* at 1127; Thomas W. Merrill, *Trespass, Nuisance, and the Costs of Determining Property Rights*, 14 J. Leg. Stud. 13 (1985). *But see* Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 Yale L.J. 1027, 1098–1103 (1995); 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).

22. The familiar two-by-two matrix of the 4 Rules of Entitlement proposed by Calabresi and Melamed is generally as follows:

Entitlement Holder↓ Level of Protection→	Property Rule	Liability Rule
Plaintiff	**Rule 1**: Plaintiff gets Injunction against Defendant's Pollution or Trespass	**Rule 2**: Defendant's Trespass/ Pollution is Allowed, but Damages are Paid to Plaintiff
Defendant	**Rule 3**: Defendant's Trespass/Pollution is Allowed (i.e., Injunction is Denied)	**Rule 4**: Plaintiff gets Injunction against Defendant's Trespass or Pollution, but Must Pay Damages to Compensate Defendant

Calabresi & Melamed, *supra* n. 20.

23. *See Intel Corp.*, *71* P.3d at 331 (Mosk, J., dissenting) ("By upholding Intel's right to exercise self-help to restrict Hamidi's bulk emails, they concede that he did not have a right to send them through Intel's proprietary system.").

California Supreme Court emphasized, Intel could exercise its right to self-help to keep Hamidi out. When self-help fails (and minds might differ on whether Intel duly exercised self-help in this particular situation), however, the law will not intervene unless and until Intel could establish actual physical impairment of its property.

In sum, although Ken Hamidi wins the lawsuit, the court by no means grants him an entitlement to send his mass emails through Intel's server; it remains the case that Intel is free to exercise self-help to keep Hamidi out. *Intel* thus appears to create some sort of hybrid entitlement or right,[24] which depends critically on the ability to exercise self-help. Self-help is not simply a discretionary choice, whereby the plaintiff could elect to exercise self-help in lieu of seeking damages or an injunction to protect his entitlement. Here, it is a stand-alone remedy, offered in a situation where the claim to protect the entitlement via injunction fails.

Tort theorists, it is fair to say, have spent little time contemplating self-help. As a starting point, then, we might look across the boundary in the realm of property (and

---

Henry Smith makes a similar point, but takes it in a different direction—namely, to point out that asymmetry writ large in the Calabresi-Melamed framework:

> As Justice Mosk pointed out in dissent, Intel did use self-help against Hamidi's emails, and the majority found that permissible; Hamidi therefore had no right to have his e-mails reach the employees through Intel's system. Thus, Hamidi is like the polluter in Calabresi and Melamed's Rule 3 scenario; the victim is denied an injunction but the injurer has no right to an injunction to force the victim to accept the unwanted pollution or e-mail. Again, the potential entitlements in the two parties are not symmetric. The reason they are not is that delineation cost is saved by simply allowing general privileges to kick in where the victim's right to exclude peters out. The victim's own privileges to act in self-help (here Intel's technical countermeasures) may or may not be effective in countering the injurer's exercise of privilege, but none of this is an occasion for legal intervention.

Henry E. Smith, *Self-Help and the Nature of Property*, 1 J.L. Econ. & Policy 69, 97 (2005). But, *contra* Smith, the entitlement here—to pollute—is really a stand-in for the factory's right to continue production activities, which is entitled to greater protection (backed by the force of law) than Hamidi's right to send his emails via Intel's server.

24. A variety of hybrid property/liability rules have been discussed in the literature. *See e.g.* Abraham Bell & Gideon Parchomovsky, *Pliability Rules*, 101 Mich. L. Rev. 1, 53 (2002); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. Rev. 2164, 2221 (2004) (invoking "loperty" rule, crediting Bell and Parchomovsky with coining the phrase).

Similar debate has played out with respect to characterization of the incomplete privilege of necessity. Under the well-known *Vincent v. Lake Erie* rule, a shipowner may dock his ship in the dire circumstances of an impending storm (it is debated whether life must be at stake, or imminent threat to property suffices) but must pay the dockowner for the damage caused to the dock. 124 N.W. 221, 221–22 (Minn. 1910). In this context, self-help is typically seen as an exception to, or carve-out of, the property owner's entitlement.

But we might also consider instead what the privilege (or right) to exercise self-help might say about the respective entitlements of shipowner and dockowner. The debate in the literature continues: Is the shipowner's entitlement to the dock protected by a property rule or a liability rule? Some commentators have suggested that the defense of necessity in the context of trespass entails a shift from a property rule to a liability rule. The owner of the land still has the entitlement, but it is no longer protected by a rule of exclusion. Instead, the intruder who is subject to forces of necessity can "take" the entitlement without the owner's consent, but when he does so, the intruder must pay the owner damages. But if that is so, could, for example, the dockowner "take back" the right to dock by releasing the ship and paying subsequent damages?

Merrill and Smith offer an alternative "property rule" theory:

> A different way of characterizing the effect of the defense, focusing on the decision in *Ploof*, might be that the defense of necessity shifts the property rule from the landowner to the intruder, who if resisted by the landowner, could use deadly force. The plaintiff 'intruders' in *Ploof* did state a cause of action in trespass, which hints at some kind of property rule protection for those in necessity.

Thomas W. Merrill & Henry E. Smith, *Property: Principles and Policies* 442 (Found. Press 2007).

criminal) law.[25] While resort to self-help is, as a formal matter, recognized in defense of all forms of property,[26] the current state of law diverges between real and personal property. Self-help is discouraged (either by statute or common law development) in the realm of real property: "It has long been the policy of our law to discourage landlords from taking the law into their own hands, and our decisions and statutory law have looked with disfavor upon any use of self-help . . . in circumstances which are likely to result in breaches of the peace."[27] More emphatically, it has been argued that "[i]n our modern society, with the availability of prompt and sufficient legal remedies . . . there is *no place and no need for self-help* . . . ."[28]

By contrast, self-help has maintained its grip when it comes to protection of personal property. The prime example is self-help repossession by creditors authorized by Article 9 of the Uniform Commercial Code (UCC): "Unless otherwise agreed, a secured party has on default the right to take possession of the collateral," and, in taking possession, a secured party may proceed without judicial process if this can be done without breach of the peace.[29] In this realm, as Tom Merrill and Henry Smith note: "[B]y exempting self-help from due process constraints, the courts have created a *powerful incentive* for lending companies to use self-help, rather than more protective statutory mechanisms."[30] As a result, as an empirical matter, most repossessions of personal property today use self-help.

One way to reconcile the divergence of the role of self-help in the land and personal property realms is to posit that resorting to self-help is allowed (preferred?) unless it will lead to violence or a breach of the peace. Certainly, in our collective imagination, the self-help metaphor conjures up images of vigilantes taking the law into their own hands—the very antithesis of legal order. This view, moreover, is consistent with early cases that evince a desire that the invocation of legal process will quell the practice of private dueling.[31] While dueling has receded into the past, modern courts hew to the bias in favor of legal process: "[w]hen landowners have confidence in the legal system, they are less likely to resort to 'self-help' remedies."[32]

---

25. The discussion in the subsequent paragraphs draws heavily from case law and discussion in Merrill & Smith, *supra* n. 24.

26. A person in possession of property can use reasonable force "to prevent or terminate an unlawful entry or other trespass upon land or a trespass against the unlawful carrying away of tangible, movable property. . . ." Model Penal Code § 3.06(1)(a) (ALI 1985).

27. *Berg v. Wiley*, 264 N.W.2d 145, 149–50 (Minn. 1978).

28. *Id.* at 151(emphasis added) (in context of tenant in claimed lawful possession of leased premises). *But see Northfield Park Assocs. v. N.E. Ohio Harness*, 521 N.E.2d 466, 474 (Ohio Ct. App. 1987) (permitting self-help in context of commercial landlord-tenant disputes). Nonetheless, in jurisdictions that permit self-help, breach of peace remains a constraining factor.

29. U.C.C § 9-609 (2001). As Merrill and Smith report: "Given the widespread adoption of the UCC by the states, creditors have tended to rely on the UCC self-help remedy rather than statutory remedies that might trigger due process hearing requirements under *Fuentes* [*v. Shevin*, 407 U.S. 67 (1972)] or [*N. Ga. Finishing, Inc. v.*] *Di-Chem*[, 419 U.S. 601 (1975)]." Merrill & Smith, *supra* n. 24, at 438.

30. *Id.* (emphasis added).

31. *See e.g. McWilliams v. Bragg*, 3 Wis. 424, 1854 WL 3450, at *4 (1854).

32. *Jacque v. Steenberg Homes, Inc.*, 563 N.W.2d 154, 160 (Wis. 1997). *See also id.* at 161 ("Although dueling is rarely a modern form of self-help, one can easily imagine a frustrated landowner taking the law into his or her own hands when faced with a brazen trespasser . . . who refuses to heed no trespass warnings.").

The law seems on solid, uncontroversial ground in discouraging self-help where it would lead to violence or a breach of peace. However, the analysis should not end there. First, violence may not be the sole "cost" of self-help that the law wishes to discourage. And second, the converse proposition needs to be investigated: should resort to self-help be *encouraged* if it would lead to positive ends?

Each of the examples discussed thus far embraces the conventional conception of self-help as a privilege to do something that would otherwise be legally actionable in order to prevent or cure a legal wrong. For example, if one has created a nuisance on one's property, the victim could enter the land of the other to abate the nuisance. Or, if someone has stolen the victim's personal property, the victim can pursue the offender (termed "in fresh pursuit") to recapture the stolen goods. In each of these situations, self-help is a discretionary remedy—the victim can choose self-help or, alternatively, he can invoke legal remedies of damages and/or injunction.

Self-help measures could also include a variety of prophylactic measures that one might take to protect one's property that do not infringe upon anyone else's legal rights. For example, one could install sound-proof glass and sound-resistant walls in one's home in order to minimize noise intrusions from the outside, which if severe, could amount to a nuisance. Here, as in the previous conception, the exercise of self-help does not affect one's resort to legal remedies.

Self-help as a prerequisite to invoke legal process challenges the more conventional view. While not uncommon in real property law, conditioning one's entitlement to legal remedies on the exercise of self-help is exceedingly rare in tort law.[33] That said, a capacious definition of self-help could include contributory and comparative negligence within its parameters. Seen in this light, a victim cannot recover from a violation of his legally protected interest unless he has exercised reasonable care—which, in essence, is a precondition for receipt of damages or an injunction.[34] Mitigation of damages—whereby a plaintiff is foreclosed from recovery of damages that could have been reasonably avoided by the plaintiff's taking affirmative measures (e.g., seeing a doctor) after the occurrence of the injury—is another doctrine that resonates with the self-help burden on the victim.

Insistence upon the exercise of self-help can be justified on different grounds. First, the victim might be the "cheapest cost avoider" of the injury, such that it is efficient to place the burden upon the victim to take self-help measures that could, in some cases, mitigate or avoid the injury altogether. Second, a "live and let live" philosophy (such as that defining the *de minimis* threshold below which nuisances are not actionable) may govern minor injuries and inconveniences. Under this conception,

33. Indeed, it is anathema in the criminal law and intentional tort contexts, which have supplied vivid analogies to courts to resist self-help prerequisites. *Cf.* Creating Computing v. Getloaded.com, LLC, 386 F.3d 930, 935–36 (9th Cir. 2004) ("Getloaded's argument that truckstop.com could have prevented some of the harm by installing the patch is analogous to a thief arguing that 'I would not have been able to steal your television if you had installed deadbolts instead of that silly lock I could open with a credit card.' A causal chain from the thief to the victim is not broken by a vulnerability that the victim negligently leaves open to the thief.").

34. I am grateful to Ariel Porat for this point.

damages are a proxy—albeit an imperfect one—for more than *de minimis* harm; or, in other words, self-help serves as a "sincerity index" for establishing the weightiness of the legally protected interest.[35] Third, and especially relevant in cyberspace, the boundaries between public and private property are contestable. Self-help can serve as a way in which someone can "mark" his property as private—or exclude it from the public commons. Thus, in order to bring a boundary-crossing property tort claim (e.g., trespass or trespass to chattel), one must first expend some effort to stake out the boundary, oftentimes no easy feat in cyberspace.

The Internet trespass to chattels cases provide an opportunity to explore this conception of conditional self-help with a sharper focus.

II. CONCEPTUALIZING SELF-HELP IN CYBERTRESPASS DOCTRINE

To begin to conceptualize the role of self-help in cybertrespass, I explore a range of options whereby the burden of demonstrating resort to self-help is placed on the plaintiff or defendant, respectively. One approach would incorporate self-help as a threshold requirement to invoke legal process. The self-help remedy, in other words, is not a discretionary option that can be elected in lieu of pursuit of other remedies (damages and injunction), but instead, pursuit of such legal remedies is conditioned upon resort to self-help in the first instance.

A different approach would recognize liability for evasion of self-help. The cause of action would turn on avoidance through misleading or fraudulent behavior. Here, the wrong switches from the actual invasion of the property right to the evasion of the self-help fortification. Such an approach might be warranted where the underlying property right is contestable and/or uncertainty abounds with respect to demarcation of its boundaries. All of these proposals would include—but by no means be limited to—a "code based approach," namely that a system owner would need to use technical measures designed to limit access to its system.[36]

Alternatively, instead of placing an affirmative burden on the plaintiff to engage in self-help, the defendant could shoulder the burden of demonstrating positive steps taken to limit the scope of their activities, such as providing a self-help "opt-out" to any affected person.

A. Self-Help in Plaintiff's Prima Facie Case

Self-help as a prima facie element could take a variety of forms. A plaintiff might have to demonstrate some threshold amount of self-help to invoke legal process;

35. An alternative balancing solution—one that has garnered substantial scholarly support in the realm of electronic intrusions—is a nuisance-type rule. *See e.g.* Dan L. Burk, *The Trouble with Trespass*, 4 J. Small & Emerging Bus. L. 27, 53 (2000); Adam Mossoff, *Spam—Oy, What a Nuisance!* 19 Berkeley Tech. L.J. 625, 654 (2004).

36. *See e.g.* Bellia, *supra* n. 24, at 2211–13 (distinguishing code-based approach from other regulatory approaches—e.g. closed access default, notice-based approach, and commons approach). Specifically, Bellia explains that "[t]o achieve legal protection, the system owner would need to use technical mechanisms designed to limit access—essentially to 'fence' or otherwise segregate information." *Id.* at 2212. *See also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1644 (2003).

alternatively, liability might be restricted to evasion of self-help measures.

1. Threshold Prerequisite to Invoke Legal Process

Examples of self-help as a threshold requirement to invoke legal process abound in real property law: "posting laws,"[37] fencing out laws,[38] and self-help precautions required to invoke trade secret protection.[39] Self-help as a threshold prerequisite resonates with what Patricia Bellia terms a "loperty" rule:[40] namely that the "use of technical measures that are actually effective in blocking some access triggers . . . the right to injunctive relief to back the terms of access the system owner sets."[41] A threshold requirement of self-help could run the gamut from minimal exertions, such as notice postings, to more significant undertakings, such as construction of effective barriers to entry.

Richard Epstein—although he does not favor such a threshold prerequisite of self-help—has provided an apt illustration of a minimal notice approach: just as an addressee can refuse to accept mail, post a "no solicitation" sign, and ask the U.S. Postal Service not to deliver at that address, the owner of an Internet server should have the right to stop email traffic over that server.[42] In both situations, Epstein seems to believe that as long as there has been communication "to any particular person that he should not deliver any mail," then "[d]elivery, *after notice*, would count as a trespass."[43] Such notices are commonly included on websites. Southwest.com, for example, posts its user agreement and restrictions in a special code (robot.txt), which "acts as an electronic sign to unauthorized spiders and robots telling them to keep out."[44]

More significant undertakings move beyond mere provision of notice to employ

37. "Posting laws" permit anyone to hunt on rural land unless it has been posted with "No Hunting" or "No Trespassing" signs. *See e.g.* Mark R. Sigmon, *Hunting and Posting on Private Land in America*, 54 Duke L.J. 549, 584 (2004) ("Twenty-nine states currently require private landowners to post their land to exclude hunters, twenty-seven of these states by statute."). These laws impose an affirmative burden of notification on the possessor of land in order to assert the right to exclude. As Merrill and Smith note, "[i]f the owner does not make the required notification, then the right to exclude is subordinated to the customary right to hunt on land owned by another." Merrill & Smith, *supra* n. 24, at 444.

38. "Fencing-out laws are a legacy of the open-range grazing system in the West, in which cattle (primarily) were allowed to roam in search of nourishment over vast stretches of land belonging to various owners (including the federal government), and were then rounded up at the end of the season and identified by brands." *Id.*

39. Here, the nature of the protected asset is significant—trade secret is a pure bundle of information. In exchange for potentially perpetual protection, we shift the costs onto the trade secret owner of assuming the cost of providing protection. Clarissa Long has written about how various forms of intellectual property represent different strategies of protection; these strategies involve tradeoffs along different margins, including the strength of the exclusionary rights and the length of term. Long compares patent law's strong exclusionary rules, its absence of liability rules and privileges, and its relatively short term with copyright's liability rules, privileges, and longer term. *See* Clarissa Long, *Information Costs in Patent and Copyright*, 90 Va. L. Rev. 465, 517–20 (2004).

40. *See* Bellia, *supra* n. 24.

41. *Id.* at 2173. Bellia, however, emphatically rejects such a rule. *Id.* ("The law should not demand technical measures as a prerequisite to a system owner's ability to exclude unwanted uses.").

42. Br. for Cal. Empl. L. Council. as Amici Curiae Supporting Petrs., *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003) (No. S103781), 2002 Cal. S. Ct. Briefs LEXIS 64-65.

43. Richard A. Epstein, *Cybertrespass*, 70 U. Chi. L. Rev. 73, 87 (2003) (emphasis added).

44. Br. of Pl. Southwest Airlines in Response to Mot. to Dismiss at 4, *Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435 (N.D. Tex. 2004).

further means to restrict access to proprietary material:

> If companies put up websites and they want to restrict access to those websites by some technological means like having a subscription or you have to have a membership and sign up, then that is totally different because you are not publishing the information publicly to the world, you are publishing it to your select members.[45]

Setting up password protected sites effectively removes the site from the public commons and marks it as private. Less drastic measures include restricting access to websites more selectively by blocking entry through use of filtering software.

Having exercised the threshold level of self-help, plaintiffs could seek injunctive relief or money damages. The ability to monetize self-help measures could also help on the front of establishing damages. Indeed, it might promote doctrinal clarity (as discussed below in Part III) by closing the gap between "damages" required by common law trespass to chattels and "loss" under the federal Computer Fraud and Abuse Act (CFAA), which has recognized such consequential economic losses.[46]

The incorporation of self-help as a threshold requirement to invoke legal process may, at least initially, seem radical. While this factor has yet to be formalized as part of the inquiry, several courts seem to have imposed some kind of *de facto* affirmative burden on the plaintiff to have exercised self-help. The seeds of such an approach were planted in the earliest cybertrespass case, *CompuServe v. Cyber Promotions*.[47] In its decision upholding an injunction against Cyber Promotions, the court noted that "CompuServe has attempted to employ technological means to block the flow of defendants' e-mail transmissions to its computer equipment, but to no avail."[48] The court did more than simply credit CompuServe for undertaking these self-help measures; it suggested such actions were a necessary precursor to invoking legal process: "[T]he implementation of technological means of self-help, to the extent that reasonable measures are effective, is particularly appropriate . . . and *should be exhausted before legal action is proper*."[49]

Taking matters into one's own hands—at least as an initial line of defense—also seems to have played a role, albeit one left undefined by the court, in other instances of a plaintiff's successful pursuit of injunctive and legal relief. In *eBay, Inc. v. Bidder's Edge, Inc.*, eBay had used technological efforts to block BE's access to its site; only when this was unsuccessful, did eBay resort to taking legal action.[50]

The converse also holds. The court that rejected Intel's overture for injunctive relief to stop Ken Hamidi's onslaught of emails gave some indication that it was not

45. *Transcript–Afternoon Session: Internet: Place, Property, or Thing—All or None of the Above?* 55 Mercer L. Rev. 919, 945–46 (2004) (statement of Jennifer Stisa Granick, Executive Director, Center for Internet and Society).

46. *See infra* nn. 100–04 and accompanying text.

47. 962 F. Supp. 1015 (S.D. Ohio 1997). In this case, Cyber Promotions was spamming the customers of CompuServe. CompuServe sought, and was awarded, injunctive relief. *Id.* at 1023.

48. *Id.* at 1017, 1024. In addition to these technological measures, CompuServe affirmatively posted a policy denying use of its computers for bulk-email purposes (fair warning), and CompuServe requested that Cyber Promotions cease sending unsolicited bulk emails to its customers. *Id.*

49. *Id.* at 1023 (emphasis added).

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

convinced that Intel had appropriately discharged its self-help obligations.[51]

The elephant in the room here is how to specify the threshold of self-help sufficient to invoke legal process. Moreover, as the disagreement between the majority and dissent in *Intel* reveals, this is apt to be an intensely fact-bound inquiry—turning on what self-help measures are reasonable under the circumstances.[52]

2. Liability for Evasion of Self-Help

Once plaintiffs engage in self-help protective measures, the flip side is that defendants evade these prophylactic measures, often through deceptive or fraudulent behavior. In spamming cases, for example, spammers will use proxies to falsify their IP addresses and send email with false mail headers. Courts, then, might ask whether the defendant employed fraudulent methods to evade self-help measures and impose liability on that basis.

Several noteworthy cases where the plaintiff has prevailed can be seen as cases where the defendant evaded self-help. In *CompuServe*, Cyber-Promotions had engaged in a variety of such deceptive measures, such as the use of misleading domain names and false email addresses in their spam messages.[53] The *CompuServe* court was most direct here: "[W]here defendants deliberately evaded plaintiff's affirmative efforts to protect its computer equipment from such use, plaintiff has a viable claim for trespass to personal property . . . ."[54] Other courts have implied that defendant engaged in some kind of deceptive work-around of the technological self-help measures taken by the plaintiff.[55] In fact, deceptive or fraudulent circumvention techniques seem so prolific, that one wonders why fraud claims are so few and far between. In *Thrifty-Tel, Inc. v. Bezenek*,[56]

51. *Intel Corp.*, 71 P.3d at 312. The dissent, however, disagreed. *See id.* at 329 (Brown, J., dissenting) ("Intel attempted to put a stop to Hamidi's intrusions by increasing its electronic screening measures and by requesting that he desist. Only when self-help proved futile, devolving into a potentially endless joust between attempted prevention and circumvention, did Intel request and obtain equitable relief in the form of an injunction to prevent further threatened injury.").

52. At a practical level, the nature and characteristics of the plaintiff may play a significant role. Large, sophisticated companies will presumably have more self-help options at their disposal than, say, small private art schools. Providers maintaining email servers for general purpose use by their customers may have fewer self-help options than private companies whose email servers are for limited business purposes. Some self-help options may make sense for some companies, but would put others out of business.

53. According to one commentator: "This 'masking' or 'aliasing' of one's Internet address is a common practice of spammers and screen-scrapers alike and turns up in almost all of the major cases on the subject." George H. Fibbe, *Screen-Scraping and Harmful Cybertrespass after* Intel, 55 Mercer L. Rev. 1011, 1014 (2004). *See also* Steve Fischer, *When Animals Attack: Spiders and Internet Trespass*, 2 Minn. Intell. Prop. Rev. 139, 156 n. 121 (2001) ("proxy servers" can be used to mask IP addresses and avoid efforts by website owners to block access to the sites).

54. Of the three portions of the injunction in this case, the first dealt with using Compuserve's computers to send bulk email while the remaining two addressed this fraud. One enjoined Cyber-Promotions from inserting a false reference to a CompuServe account in any email of the defendant's; the second forbade them from falsely representing that any mail of theirs came from a CompuServe account. The court also noted that these two practices would be forbidden under the Lanham Act, 15 U.S.C. § 1125(a). *CompuServe Inc.*, 962 F. Supp. at 1017, 1019–20.

55. *See e.g. eBay, Inc.*, 100 F. Supp. 2d at 1062–63 (eBay's technological efforts to block scraper's access to its site were unsuccessful). *See also* Br. of Pl. Southwest Airlines, *supra* n. 44, at 6 (Southwest claimed that "defendant has evaded these website protection measures by 'masking' or hiding its identity when its robots enter and scrape Southwest.com.").

56. 54 Cal. Rptr. 2d 468 (App. 4th Dist. 1996).

the California court held defendant teenagers liable for fraud based upon their misrepresentations to the phone company's computer system (plaintiff's agent) that they were authorized users.[57]

How would *Intel* come out under this paradigm?[58] Hamidi apparently sent his emails from different computers to get around Intel security.[59] And Intel claimed that a significant amount of staff time was taken up by attempts to block Hamidi's emails.[60]

A similar elephant is present here: courts must determine the threshold point at which the evasive tactics of the defendant warrant liability. For example, in the *eBay* case, eBay had blocked over 150 IP addresses and yet, Bidder's Edge kept finding ways in.[61] Should eBay be allowed to come to court after Bidder's Edge circumvented the first IP block? More likely, that would constitute a *de minimis* evasion of self-help; but at what point would it become actionable? The inquiry here, moreover, presupposes that plaintiff has exercised self-help measures. But what is the precise relationship between the two? Namely, if plaintiff's self-help attempt is low-tech, inefficient, and unlikely to succeed, would plaintiff still have a cause of action against the defendant for its end run around the nominal self-help effort?

B. Self-Help "Opt-Out" as Affirmative Defense

A different paradigm could relieve plaintiff of any affirmative burden to engage in self-help and place the burden on the defendant to demonstrate positive steps taken to limit the scope of its activities, such as providing a self-help "opt-out" to any affected person.

In re Doubleclick, Inc. Privacy Litigation is instructive.[62] DoubleClick faced a class action lawsuit brought by computer users for using "cookies" to collect data (including personal information) from their computers that DoubleClick then used in targeted banner advertisements. The plaintiffs alleged that they suffered damage in removing Doubleclick's software from their computers. The court found that DoubleClick was insulated from liability because it provided two easy opt-out methods: "as counsel demonstrated at oral argument, users may easily and at no cost prevent Doubleclick from collecting information by simply selecting options on their browsers or downloading an "opt-out" cookie from Doubleclick's Web site."[63] In other words, the defendant in this case provided a self-help method for the plaintiff to use in order to

57. *Id.* at 473–74.

58. The factual details are murky, as this was not the framework the court adopted.

59. The court is not clear, but this implies that Intel tried IP address blocking.

60. *Intel Corp.*, 71 P.3d at 301 (noting that Intel presented "uncontradicted evidence . . . that staff time was consumed in attempts to block further messages from FACE-Intel.").

61. *eBay, Inc.*, 100 F. Supp. 2d at 1068.

62. 154 F. Supp. 2d 497 (S.D.N.Y. 2001). While there was a trespass claim in this case, the court did not address it because all federal claims were eliminated and thus the district court lacked jurisdiction. *Id.* at 526. A CFAA violation was also alleged. Plaintiffs' claims, however, were largely dismissed for failure to allege sufficient damages or loss (amounting to the $5000 threshold). *Id.* at 519–26. There were hearings on a proposed final judgment/settlement. The court ordered that the complaint be dismissed and the settlement was approved. No. 00-CIV-0641 (NRB), 2002 U.S. Dist. LEXIS 27099 (S.D.N.Y. May 23, 2002).

63. *In re Doubleclick, Inc.*, 154 F. Supp. 2d at 524.

avoid damage, and thus could not be held liable to those who failed to take advantage of it.[64]

Hamidi, too, included an "opt-out" in his emails and did not send further messages to anyone who opted out. Hamidi, even if he was evading the Intel spam filters, identified himself and his cause.[65] And while the "opt-out" was directed to the individual employee email users, Intel could have instructed its employees to opt-out.

III. EXISTING CYBERTRESPASS DOCTRINE IN DISARRAY

Instead of relying upon a rigid, some might say arcane, doctrinal requirement of damage to physical chattel, the self-help approach would substitute the concepts of some sort of affirmative threshold burden on the plaintiff to demonstrate reasonable self-help measures or defendant's deceptive evasion of those prophylactic self-help measures; or else place an affirmative burden upon the defendant to secure a reasonable "opt out" for plaintiff. Such an approach would contribute clarity and coherence to cybertrespass doctrine, which is marked instead by confusion and indefensible line-drawing.

Intel set the stage for a rash of electronic intrusion cases. Thus far, the doctrinal development of the trespass to chattels tort in this new context has focused upon how to define harm or damage to the chattel. The type of harm, ranging from actual physical damage to the computer server or network to consequential economic harms from loss of consumer goodwill and employee productivity, is typically outcome determinative.

If the common law "damage" requirement has proved overly restrictive in some cases, and ultimately theoretically bankrupt, the alternative standard of "loss" ushered in by the CFAA is overly broad, leading to the grant of injunctions in situations where parties have weak claims to property rule protection in arenas focused on the dissemination of information. The self-help approach emerges as a favorable compromise position between these two extremes.

A. Common Law Trespass to Chattels Claims

Courts facing trespass to chattels claims have tended to focus on how to define "harm" or "actual damage" to the chattel. The *Restatement* includes within its definition of harm: dispossession or deprivation of the chattel; impairing the "condition, quality, or value" of the chattel; or harm to "some person or thing in which the possessor has a legally protected interest."[66] Just what constitutes sufficient harm in the context of

64. Laws in European and other countries require companies to get affirmative "opt in" approval before collecting customer information. *See e.g.* Robert Gellman, *Privacy: Finding a Balanced Approach to Consumer Options* 36, Center for Democracy & Technology, http://www.cdt.org/privacy/ccp/consentchoice4.pdf (2007) ("Many countries require clear and affirmative consent before permitting any secondary use of sensitive personal information . . . . Consumers should always be able to exercise choice free of charge. Consumers have that right by law in Europe and in other countries.").

65. Hamidi can thus be contrasted profitably with defendants such as the one in *Sch. of Visual Arts v. Kuprewicz*, 771 N.Y.S.2d 804 (N.Y. Sup. Ct. 2003). In that case, plaintiff alleged that the defendant signed its human resources director up on lists to receive pornographic email spam and posted a number of false job advertisements on Monster.com. Although in this case the court did not mention self-help measures at all, there is an interesting distinction between this case and *Intel*—namely, the fraudulent nature of the spamming.

66. Section 218 of the *Restatement (Second) of Torts* reads in full:

electronic intrusions to email servers and web servers has been the subject of much debate. The law here is very much in flux.

1. Impairment of a Computer Server

The strictest interpretation of harm approximates a "physical harm" requirement. It hews closely to the *Restatement's* explanatory comment: "one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the *physical condition*, quality, or value of the chattel."[67] The prime analogue to physical harm in the context of the Internet is the impairment of the functioning of email and web servers (as opposed to actual physical damage to the computer equipment). Just precisely what constitutes such impairment, however, is the subject of some disagreement.

In *CompuServe*, the court stressed that the electronic intrusions consumed disk space and drained processing power, the effect of which was to diminish "the value of that equipment" to its owner.[68] *Intel* embraced this conception of harm and several courts have followed suit.[69]

There is some potential leeway with respect to the magnitude of the infringement upon server capacity, namely how significant a portion of the server must be disabled for authorized users.[70]

Moreover, the issue may be slightly different when a web server (as opposed to a mail server) is at issue. In the context of web servers, some courts have seemed more

---

One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

(a) he dispossesses the other of the chattel, or
(b) the chattel is impaired as to its condition, quality, or value, or
(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.

Restatement (Second) of Torts § 218.

67. *Id.* § 218 cmt. e (emphasis added).

68. *Compuserve, Inc.*, 962 F. Supp. at 1022 ("To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.").

69. *Intel Corp.*, 71 P.3d at 300 (refusing to recognize "an electronic communication that neither damages the recipient computer system nor impairs its functioning"). *See e.g. Sch. of Visual Arts*, 771 N.Y.S.2d at 808 (recognizing actionable trespass to chattels where unsolicited emails "depleted hard disk space, drained processing power, and adversely affected other system resources on [plaintiff's] computer system") ("[T]his Court's decision . . . is not based upon the content of the e-mails, but rather, is predicated upon plaintiff's allegation that its receipt of large volumes of e-mails have caused significant detrimental effects on [the art school's] computer systems.").

70. *See e.g. Tyco Intl. (US) Inc. v. John Does*, 2003 WL 23374767 at *4 n.3 (S.D.N.Y. Aug. 29, 2003) ("Tyco's allegation that the e-mail attack rendered a significant portion of the Tyco server unavailable for authorized users suggests that the value of the server was probably diminished in some measurable way."). (It is worth pointing out that the court's statement here is dicta, as Tyco did not actually make a claim for compensatory damages. Instead, Tyco sought—and was awarded—punitive damages for the spammer's "willful and wanton" acts. *Id.* at *4.); *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 WL 388389 at *7 (N.D. Cal. Apr. 16, 1998) ("[D]efendants trespassed . . . thereby filling up Hotmail's computer storage space and threatening to damage Hotmail's ability to service its legitimate customers . . . .").

inclined to credit a lower threshold of harm,[71] whereas others have held fast to the stricter definition at play in the mail server cases, namely impairment of the functioning of the server (in addition to unauthorized access by the intruder).[72]

On this point, clear rules are in short supply. On the one hand, the *Intel* bottom line—the requirement of physical harm to, or functional impairment of, mail or web servers—stands as a potentially formidable barrier in electronic intrusion cases. Indeed, *Intel* is an apt stand-in for the difficulties inherent in establishing the requisite harm (at least in the realm of email servers). The California Supreme Court was adamant that the trespass to chattels tort "does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning."[73] That said, on the other hand, the concept of impairment of server capacity is potentially more malleable. Indeed, as the Fifth Circuit Court of Appeals warns in a recent case, *White Buffalo Ventures, LLC v. University of Texas*: " '[s]uffer the servers' is among the most chronically over-used and under-substantiated interests asserted by parties . . . involved in Internet litigation . . . ."[74]

2. Threat of Potential Future Harm

A more expansive conception of harm incorporates the threat of potential future harm. *eBay, Inc. v. Bidder's Edge, Inc.* was the first to recognize future harm, in a case involving the use of "spiders," or web crawlers, to conduct automatic recursive searches of a competitor's website.[75] Although the spiders' infringement upon web server space could be considered *de minimis*, the court not only credited it as harm,[76] but also made clear that:

> Were [the court] to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to

71. *See e.g. eBay, Inc.*, 100 F. Supp. 2d at 1071 ("Even if, as [Bidder's Edge] argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes . . . . BE's actions appear to have caused injury to eBay and appear likely to continue to cause injury to eBay.").

72. *See e.g. Ticketmaster Corp. v. Tickets.Com, Inc.*, 2003 WL 21406289 at *3 (C.D. Cal. Mar. 7, 2003) ("Since the spider does not cause physical injury to the chattel, there must be some evidence that the use or utility of the computer (or computer network) being 'spiderized' is adversely affected by the use of the spider. No such evidence is presented here."); *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326, 354 (D. Me. 2003) ("[E]ven assuming *arguendo* that [the defendant] did access Pearl's network without authorization, there is no evidence that in so doing he impaired its condition, quality or value.").

73. *Intel Corp.*, 71 P.3d at 300.

74. *White Buffalo Ventures, LLC v. U. of Tex.*, 420 F.3d 366, 375 (5th Cir. 2005). For this reason, the court cautions against "declaring server integrity to be a substantial interest without evidentiary substantiation," and emphasizes that "rules imposed pursuant to such interests require more than a judicial rubber-stamp." *Id.* at 377, 375. The court "respectfully disagree[d] with other district courts' finding that mere use of a spider to enter a publicly available web site to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels." *Id.* at 377 n. 24 (quoting *Ticketmaster Corp.*, 2003 WL 21406289 at *4).

75. 100 F. Supp. 2d at 1073.

76. *Id.* at 1064, 1066 n.14 (stating that the Bidder's Edge spiders occupied up to 1.53% of the total load on eBay's servers). The court held that this infringement, nonetheless, was actionable because it "deprived eBay of the ability to use that portion of its personal property for its own purposes." *See id.* at 1071. Moreover, despite the small load, the robot queries "diminished the quality or value of eBay's computer systems." *Id.*

> crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value.[77]

The concept of "threat of future harm" has not yet crystallized in the courts. A key issue pertains to the kind of showing required to demonstrate that others will replicate the infringer's activity. Thus far, courts have acted as if they "know it when they see it." For example, in *Register.com, Inc. v. Verio, Inc.*,[78] the court seemed confident that "if [defendant] were permitted to continue to access [plaintiff's] computers through such robots, it was '*highly probable*' that other Internet service providers would devise similar programs to access [the plaintiff's] data, and that the system would be overtaxed and crash."[79]

But distinguishing the dangerous slippery slope situations from the one-off infringements is a precarious game.[80] It is also somewhat unclear whether the threat of potential future harm can substantiate a claim for actual present damages as opposed to injunctive relief and, if so, how one would go about quantifying the harm.[81] Finally, to date, the threat of future harm has been recognized only in the web server cases, so it is unclear whether the rationale would have force in the mail server context.

3. Consequential Economic Losses

In addition to actual—or threatened—damage to the functioning of the computer servers, a minority of cases have credited consequential economic losses. Does the system owner have a "legally protected interest" against these?

Several courts have considered harm to business reputation and goodwill. These cases typically are brought by Internet Service Providers (ISPs) for interference with their ability to provide efficient service to their legitimate customers.[82] The *CompuServe* court was perhaps most resolute: "[m]any subscribers have terminated their accounts specifically because of the unwanted receipt of bulk e-mail messages. Defendants' intrusions into CompuServe's computer systems, insofar as they harm plaintiff's business reputation and goodwill with its customers, are actionable under Restatement

77. *Id.* at 1071–72.

78. 356 F.3d 393 (2d Cir. 2004). In this case, Verio used an automated robot to download customer information from a competitor's (Register.com) website and then used that information to solicit the competitor's customers.

79. *Id.* at 404 (emphasis added). *See also* Temp. Inj. at 2–4, *Am. Airlines, Inc. v. Farechase, Inc.*, No. 067-194022-02 (67th Dist. Ct., Tarrant County, Tex. Mar. 8, 2003) (available at http://w2.eff.org/legal/cases/AA_v_Farechase/20030310_prelim_inj.pdf (last accessed Aug. 23, 2009)) (enjoining defendant from using a screen-scraper to compile data from American Airline's website, relying, in part, on the fact that, absent an injunction, other scrapers would jump into the fray and burden American's website).

80. In *Ticketmaster Corp.*, 2000 WL 1887522, for example, the court refused to issue a preliminary injunction against a company engaged in screen-scraping. According to the court, unlike in *eBay*, there was no likelihood of "dozens or more parasites joining the fray." *Id.* at *4.

81. For example, in *Phys. Interactive v. Lathian Sys., Inc.*, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003), the court held that plaintiff had shown irreparable harm by "the costs it must incur to guard against future attacks." *Id.* at *9. In this case, plaintiff had sought a preliminary injunction and thus was required to demonstrate "irreparable harm." *Id.* at *4.

82. At its core, this type of action brought by the ISP provider for its own economic losses might be reconceptualized as, in essence, allowing the ISP provider to act akin to a class action plaintiff on behalf of its members.

§ 218(d)."[83]

This "loss of consumer goodwill" rationale—often coupled with diminished employee productivity due to the need to "sort through and respond to the misdirected e-mails"[84]—has succeeded in several successor ISP spamming cases.[85] But often the consequential economic harm to reputation, goodwill, and employee productivity is aggregated with the more concrete impairment of server efficiency. In fact, such consequential economic harms have been recognized (thus far) exclusively as one piece of an aggregated harm.[86]

B. Federal Computer Fraud and Abuse Act (CFAA) Claims

The Computer Fraud and Abuse Act (CFAA)[87] adds a federal overlay to doctrinal development in the law pertaining to electronic intrusions.[88] Originally enacted exclusively as a criminal statute,[89] the CFAA was amended in 1994 to add a private civil cause of action with fairly broad jurisdictional reach.[90] Although most often

---

83. *CompuServe Inc.*, 962 F. Supp. at 1023 (citation omitted). Recall that *Restatement (Second) of Torts* § 218 (d) refers to "bodily harm [that] is caused to the possessor, or harm [that] is caused to some person or thing in which the possessor has a legally protected interest."

Patricia Bellia makes the astute point that "[b]y subtly shifting its focus from CompuServe's *servers* to its *service*, the *Intel* 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." Bellia, *supra* n. 24, at 2183 (emphasis in original).

84. *Hotmail Corp.*, 1998 WL 388389 at *7. The diminishment of employee productivity rationale was rejected in *Intel Corp.*, 71 P.3d at 307–08.

85. This argument was pressed by another ISP, America Online (AOL), in a pair of cases. A federal district court in Virginia held that plaintiff, who sent bulk e-mail messages, "injured AOL's business goodwill and diminished the value of its possessory interest in its computer network." *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (concluding that "[t]here is, therefore, no factual dispute as to whether [plaintiff] committed a trespass to chattels against AOL's computer network"). *See also Am. Online, Inc. v. LGCM, Inc.*, 46 F. Supp. 2d 444, 452. (E.D. Va. 1998) (recognizing damage to AOL's corporate goodwill from bulk emailers); *In re Am. Online, Inc.*, 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001) (analogizing harm to ISP provider, which claimed damages under the CFAA for software installed by AOL on the computers of ISP's customers, to loss of corporate goodwill in *AOL v. LGCM*).

86. *See e.g. Hotmail Corp.*, 1998 WL 388389 at *7 (specifying that harm from unsolicited bulk emails included "filling up Hotmail's computer storage space and threatening to damage Hotmail's ability to service its legitimate customers," "added costs for personnel to sort through and respond to the misdirected e-mails," and "harm to Hotmail's business reputation and goodwill."). *See also Register.com, Inc.*, 126 F. Supp. 2d at 252 (recognizing damages under trespass to chattels as a combination of "costs relating to repair and lost data and also . . . lost good will based on adverse customer relations").

87. 18 U.S.C. § 1030 (2008).

88. This federal overlay raises a much broader issue (beyond the scope of this article)—namely, given the existence of the federal civil cause of action under the CFAA, how should we conceive of the role of the common law tort of trespass to chattels?

89. More specifically, the Act was directed at protecting classified information on government computers and sensitive information on financial institution computers. *See* 18 U.S.C. § 1030(e)(2)(A). The Amendments broadened its purview to all computers used in interstate commerce. *See* Sen. Rpt. No. 104-357 at 10 (Aug. 27, 1996) (available at 1996 WL 492169) ("Senator Leahy was the principal sponsor of the 1994 amendment to subsection 1030(a)(5), which was intended to broaden the reach of the provision by replacing the term 'federal interest computer' with the term 'computer used in interstate commerce or communication.' "); 18 U.S.C. § 1030(e)(2)(B) (currently defining "protected computer" as one "used in or affecting interstate or foreign commerce or communication").

90. *See* Sen. Rpt., *supra* n. 89, at 11–12, 14 ("The amendment to section 1030(g) provides that victims of computer abuse can maintain a civil action against the violator to obtain compensatory damages, injunctive relief, or other equitable relief.").

characterized in its civil guise as an anti-hacking statute, the CFAA has been interpreted much more expansively.[91]

While for some time—notwithstanding the scholarly attention devoted to emerging common law trespass to chattels actions—the CFAA has ducked under the radar screens of most (including Richard Epstein), recognition of its significance is taking hold.[92] It has been described by one commentator as the "federal analogue" to common law trespass to chattels in the context of the Internet.[93] The CFAA provides a civil action for damages or injunctive relief to anyone who has suffered "damage *or loss*" as a result of someone who intentionally accesses a computer without authorization or exceeds authorized access, so long as the conduct involved an interstate or foreign communication.[94] Most (but not all) cases that assert a trespass to chattels claim that occur after 1994 (when the civil suit provision of the CFAA was enacted[95]) have included a CFAA claim as well.

CFAA claims share many similarities with common law trespass to chattels claims, but there are also important differences. To begin, there are some built-in limitations. To invoke the CFAA, a plaintiff must establish "unauthorized access" to a computer.[96] There are also several jurisdictional prerequisites. The conduct must involve an interstate or foreign communication.[97] In addition, plaintiff's economic damages must exceed $5,000.[98] And, unlike in the trespass to chattels context, damages are limited to

91. While the CFAA is concerned with hacking, it is not limited to cases in which an individual has manipulated a computer program outside its intended function. It also covers cases where, for instance, an individual has accessed a computer for which they possessed sufficient log-on information, but used the computer in violation of specified terms of use. *In re American Online, Inc.*, 168 F. Supp. 2d 1359 (S.D. Fla. 2001), is illustrative of the breadth of coverage. In that case, AOL allegedly distributed "defective" software in its AOL 5.0 revision. *Id.* at 1365. The claimed violation—under both the CFAA and tortious interference with customers—was that the software "took over" the computer by hiding certain system settings and disrupting communications with other ISPs. *Id.* The court upheld two of the CFAA claims on behalf of customers and ISP providers (but dismissed the tortious interference claims). *Id.* at 1381–82.

92. According to one practitioner, the CFAA "is fast becoming one of the most expansive and potent civil statutes in a civil litigator's arsenal." Nick Akerman, *CFAA Resembles RICO*, 27 Natl. L.J. 13, 13 (Aug. 29, 2005) (available on Westlaw at 8/29/2005 Natl L.J. 13).

93. Bellia, *supra* n. 24, at 2197.

94. 18 U.S.C. § 1030(g) (emphasis added).

95. *See supra* n. 90 and accompanying text.

96. 18 U.S.C. § 1030(e)(10). Courts have broadly interpreted this "unauthorized access" requirement. Significantly, they have credited a computer owner or operator's restrictive "terms of use" provisions as setting the scope of authorized use of the computer or underlying data. *See e.g. EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access."); *Register.com, Inc*, 126 F. Supp. 2d at 245 (granting injunction to plaintiff based in part upon Verio's concession that "it [had] violated Register.com's posted restriction on the use of . . . data for direct mail and telephone marketing purposes"), *aff'd on other grounds*, 356 F.3d 393 (2d Cir. 2004); *S.W. Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) (finding plaintiff had sufficiently alleged "unauthorized access" based on website terms of use that "prohibited the use of 'any deep-link, page-scrape, robot, spider or other automatic device, program, algorithm or methodology which does the same things'"); *Bus. Info. Sys. v. Prof. Govtl. Research & Solutions Inc.*, 2003 WL 23960534 at *7 (W.D. Va. Dec. 16, 2003) ("[I]f [plaintiff] wanted to restrict its users in their abilities to make unfettered use of the records they were accessing, then it could have done so easily through its terms and conditions of usage . . . .").

97. 18 U.S.C. § 1030(e)(2)(B). This is not a particularly demanding jurisdictional criterion. Most computers that send email across state lines will qualify.

98. *Id.* § 1030(a)(5)(B)(i) ("loss . . . during any 1-year period . . . aggregating at least $5,000 in value"). The 2000 Amendments to the Act retained the $5,000 jurisdictional threshold, rejecting a competing bill that would have eliminated it:

economic harms; punitive damages are specifically prohibited.[99]

But, along the harm dimension, the CFAA is more liberal, or expansive, than common law trespass to chattels doctrine; whereas the common law fixates on actual damage, the CFAA defines harm as "damage *or loss*."[100] "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information."[101] The definition of "loss" sweeps much more broadly to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[102]

Losses are thus defined broadly to include expenses due to interruption of service as well as the costs of responding to the attack.[103] Recovery of damages under the CFAA, unlike under common law trespass to chattels, is not restricted to damage to the chattel, and easily encompasses consequential damages such as loss of goodwill or consumer satisfaction. The CFAA definition might even be stretched to include the cost

---

> Specifically, as introduced, S. 2448 would have over-federalized minor computer abuses. Currently, federal jurisdiction exists for a variety of computer crimes if, and only if, such criminal offenses result in at least $5,000 of damage . . . . S. 2448, as introduced, would have eliminated the $5,000 jurisdictional threshold and thereby criminalized a variety of minor computer abuses, regardless of whether any significant harm resulted.

146 Cong. Rec. S10915 (Oct. 24, 2000) (statement of Sen. Leahy).

99. 18 U.S.C. § 1030(g). Thus, state common law claims retain significance where noneconomic or punitive damages are at issue. *See e.g. Creative Computing v. Getloaded.com L.L.C.*, 386 F.3d 930, 933 (9th Cir. 2004) (state trade secrets law used to provide exemplary damages for willful misconduct).

100. The definition of "damage" was separated from "loss" via the Patriot Act in 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, § 814(d)(5), 115 Stat. 272 (2001). Prior to then, loss was included within the definition of damage. The scant extant legislative history provides a clue into the impetus for disentangling damage from loss:

> The 1994 amendment required both "damage" and "loss," but it is not always clear what constitutes "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no "damage," the victim does suffer "loss." If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.

Sen. Rpt., *supra* n. 89, at 11–12.

101. 18 U.S.C. § 1030(e)(8).

102. *Id.* at § 1030(e)(11).

103. *See e.g. Pacific Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1197 (E.D. Wash. 2003) (defining loss to include costs required to "mak[e] a company's computer database more 'hacker-proof,' " as well as costs of hiring computer forensic expert to investigate the attack). Courts have addressed various issues including whether such costs can include the costs of responding to threats that could have been avoided by prior (cheaper) preventative measures (*see e.g. Creative Computing*, 386 F.3d at 935–36 (determining that damages can include repair and recovery activities that could have been avoided by cheaper preventative measures prior to the damage)), or costs to combat the threat of future attacks (*see e.g. U.S. v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000) (in an appeal from a criminal conviction under CFAA, interpreting damages to include "making the system as secure as it was before, not making it more secure than it was before")).

of various "self-help" measures.[104]

EF Cultural Travel BV v. Explorica, Inc.,[105] a major screen-scraping case, is instructive. In that case, Explorica, a competing tour company formed by several former employees of EF Cultural Travel (EF),[106] hired a software firm to develop a screen-scraping tool to mine EF's website for tour pricing information.[107] Explorica used this price information to undercut EF's prices for its competing business. The district court granted a temporary injunction (later upheld by the court of appeals), finding that EF was likely to prevail on the CFAA claim.[108] Moreover, damages included not only damage to their systems (which was minimal), but also loss of customers. Indeed, the court explained that limiting damages to physical effects would (in addition to contravening Congress' intent) "serve to reward sophisticated intruders."[109] Even more expansively, plaintiff was awarded damages for the costs of investigating the source of the intrusion, given that the investigation was necessary in order to fix the chattel and/or prevent future attacks.[110] The court emphasized, "[a]s we move into an increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim of what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger."[111]

An even more creative definition of "loss" under the CFAA was employed by the court in *America Online, Inc. v. National Health Care Discount, Inc.*[112] In this spamming case, the court held that National Health Care Discount violated both common law trespass to chattels and the CFAA. The court calculated damages in an unorthodox manner: it based its calculation upon the amount of free advertising received by the defendant, as opposed to impairment to the system.[113]

---

104. *See e.g. Tyco Intl. (U.S.), Inc*, 2003 WL 23374767 at *3 (damages can include losses due to the costs of investigation needed to prevent further attacks).

105. 274 F.3d 577 (1st Cir. 2001).

106. One key element of the *Explorica* case is its method of establishing the CFAA statutory definition of unauthorized access. Access under the CFAA was unauthorized because the former EF employees had signed confidentiality agreements with EF and used this confidential information to create the scraper. *Id.* at 582 (finding unauthorized access "based on the confidentiality agreement" between EF and the former employees who orchestrated the download); *id.* at 583 ("[I]f proven, Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website.").

107. They used a scraper tool to download automatically (via EF's publicly available website) all of EF's prices for high school tours. This information could ordinarily be taken off the website, but only one piece of information at a time. *Id.* at 579–80, 580 n. 3.

108. Plaintiff did not bring a common law trespass to chattels claim.

109. *Explorica*, 274 F.3d at 585.

110. *Id.* at 584–85 (" '[L]oss' would fairly encompass a loss of business, goodwill, and the cost of diagnostic measures."). As one court commented: "[T]he *Explorica* decision demonstrates the ease with which a plaintiff may be able to satisfy . . . the $5,000 damages element." *P. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1197 (E.D. Wash. 2003).

111. *Explorica*, 274 F.3d at 585.

112. 174 F. Supp. 2d 890 (N.D Iowa 2001).

113. In reaching this determination, the court brokered a compromise between two proposed damages standards: (i) the fixed cost of delivering the determined number of bulk emails (roughly $0.78/1000) and (ii) the cost of an equivalent number of banner adds (roughly $8.50/1000). The court, in essence, split the difference in arriving at the $2.50/1000 calculation. *See id.* at 901 ("The court concludes that while an award of 78¢ per thousand pieces of NHCD's [unsolicited bulk email] sent to AOL members would not adequately compensate AOL for its damages, $8.56 per thousand pieces of UBE would dramatically over-compensate

IV. THE NORMATIVE APPEAL OF THE HYBRID SELF-HELP APPROACH

The self-help approach is a compromise or hybrid approach located between two poles: the doctrinal status quo represents one end of the spectrum, characterized by a harm-based approach; Richard Epstein's proposed trespass to land, or "property rule" approach is situated at the opposite end.

Amidst the murkiness of present doctrine and theory, Epstein, as usual, offers clarity. He has argued forcefully that the law's "acceptance of self-help establishes that the owner [or possessor] of the chattel has an exclusive right to use it as he sees fit."[114] Epstein defends a strong, absolute property rights position—a "property rule" in Calabresi-Melamed parlance—that accords the right of the owner/possessor of the property to enjoin its use regardless of whether any harm to the property has occurred. The rules of trespass to property, he believes, "carry over to cyberspace without missing a beat."[115] Consistent with these views, Epstein argued in *Intel*[116] that a trespass to chattels claim does not demand a showing of harm to the chattel if damages are not sought. Epstein has asked: "why stick to the rule that requires a proof of actual damages in order to obtain injunctive relief"[117] and "why deny a legal remedy when the self-help remedy turns out to be inadequate?"[118] Epstein, in other words, hews to the conventional view of the self-help remedy as discretionary; a victim may elect either to take matters into his own hands or seek injunctive relief. And, if a victim has the right to self-help, it follows that he also has a right to seek legal remedies for protection.[119]

In this article, I have proposed a different conception of the self-help remedy as a precondition for invoking legal enforcement. Self-help stands as the "missing third remedy" not simply as a substitute for property rule protection. And, in some situations where a victim has a right to engage in self-help, failure to do so will foreclose injunctive relief. Cybertrespass claims are a good case in point, where, given certain features of the legal landscape in cyberspace, the hybrid self-help approach has normative appeal.

AOL."). In any case, the court's determination seems wholly unrelated to the CFAA damages standard.

114. *See* Epstein, *supra* n. 6, at 151; Epstein, *supra* n. 43, at 75.

115. Epstein, *supra* n. 43, at 81.

116. Epstein wrote an amicus curiae brief on behalf of industry groups such as The California Employment Law Council in support of Intel, which was discussed and ultimately rejected in the court's opinion. *See* Br. for Cal. Empl. L. Council, *supra* n. 42, at 39. For the court's discussion of Epstein's brief, *see Intel Corp. v. Hamidi*, 71 P.3d 296, 309–10 (Cal. 2003). Epstein also wrote an amicus brief in *eBay, Inc.*, making similar arguments. *See* Epstein, *supra* n. 43, at 80.

117. Epstein, *supra* n. 6, at 151.

118. *Id.*

119. Epstein has elaborated:

> The dominant feature of any self-help strategy is that it pairs a quick, cheap and reliable remedy with *incomplete* relief, that is, relief which by definition and design does *not* leave the aggrieved party as well as he would have been if the other party had faithfully performed its obligations in the first place. Here, there is no obvious reason why the law should *deny* any private party the option of using that self-help remedy. Rather, what the law should do is to supply a second legal remedy that offers the complete relief (or at least more complete relief) that the self-help remedy could not supply. At this point, the aggrieved party has a choice. If he chooses self-help, then never force him to make a higher investment in legal costs to secure a superior form of remedy. If he chooses to incur greater legal expense for a greater return, that is fine. Thus, the public system supplies an extra option, not an obligation.

Epstein, *supra* n. 17, at 26 (emphasis in original).

A. Self-Help as Sincerity Index

The self-help approaches—particularly the ones that place an affirmative burden on the plaintiff—function as a sort of significance or sincerity index. In the digital context, self-help is a signal to the world (and the law) that one is asserting a property right. "[S]harp boundary conditions" are a prerequisite in Epstein's world for the "eas[e of] determin[ing] what actions count as a violation of th[e] rule [against physical invasion of the space of another]."[120]

Requiring that the signal be costly to implement—the costs, for example, of including a self-help code—operates as an indication of the victim's sincerity. It will not suffice simply to slap a "do not copy" at the top and bottom of a web page and thereby get protection. This makes it more akin to "No Hunting" signs—because it is somewhat costly to put these up, we know the property owner is serious about not wanting hunters on the land.

Epstein himself seems to have endorsed (at least implicitly) a very weak form of such a rule with his analogy in *Intel* of the "no solicitation" sign.[121] But, Epstein also insists—naively in my view—that simply caring enough to bring suit sufficiently demonstrates one's sincerity and implies that significant loss has been incurred by the plaintiff:

> If eBay or Intel had suffered only nominal damages, then why would either firm spend enormous sums of money in order to stop conduct that at some level they regarded as deleterious to their businesses? The central insight in the economics of litigation is that no plaintiff will sue to recover when the costs of litigation exceed the expected recovery of suit. . . . We do not have to estimate in the abstract how substantial these damages are because we have a perfect case of revealed preferences. The willingness of firms to sue in order to defend the exclusive use of their own space is evidence enough that the damages count.[122]

Epstein's view refuses to contemplate that some of the gains sought by bringing a lawsuit might have economic value to plaintiff, but would be considered illicit in a social cost-benefit calculus—such as a desire to stifle a particular party's speech or viewpoint. But it also overlooks the fact that companies could well have strategic business reasons, including forestalling competitors, that could motivate them to seek cheap or easy injunctive relief. So, for example, an airline company offering prices and various services online for the entire public could foreclose a competitor from having access to its information, along with that of other competitors, in order to aggregate information for consumers. And, wielding the CFAA, it could do so, notwithstanding any "damage" to its server website and without taking any steps, for example, to circumscribe access to its site only to password protected potential consumers.[123]

---

120. *Id.* at 18.

121. *See supra* text accompanying n. 42–44.

122. *See* Epstein, *supra* n. 43, at 78, 81–82 ("No one in his right mind sues for nominal damages. The litigation costs of such a noble undertaking dwarf the pitiful recovery even if the suit is certain to succeed . . . . The law in its infinite wisdom has denied a cause of action that no rational person has ever wished to bring").

123. Several airlines have received injunctions via CFAA claims. *See e.g.*, Temp. Inj. at 2–4, *Am. Airlines, Inc. v. Farechase, Inc.*, No. 067-194022-02 (67th Dist. Ct., Tarrant County, Tex. Mar. 8, 2003) (available at

B. Self-Help as Boundary Marker

The affirmative self-help burden also serves as a boundary marker, putting others on notice of the property interest at issue. This boundary-fixing role has historical roots. In medieval times, trespass to land actions served not only to protect ownership and the public order, but also to fix property boundaries.[124] This role takes on particular significance in cyberspace, where there are recurrent debates surrounding the "propertization" of the Internet and disputes as to what should be considered the public commons versus private property.[125] Trespass to chattels claims, then, serve to determine otherwise fuzzy boundaries and entitlements on the Internet. By expending efforts in taking self-help measures, a party can effectively remove property from the public commons and tag it essentially as private property. What a party cannot do is refuse to cordon off its website from the commons, benefit from all the upside of being accessible by the general public, but then protect itself from any downside—whether by way of unwanted communication or increased competition—by selectively seeking to keep certain users out.

Here, too, Epstein would agree with the general principle, if not with its particular application in cyberspace.[126] As an economic matter, provision of notice reduces the avoidance cost of third parties. Self-help may serve as cost-effective way to notify third parties, who are unfamiliar with the asset and the boundaries of the property. Marking is a requirement in patent law and other rules in copyright play a similar notice function.[127]

One can find traces of this idea in the case law. In both *Southwest Airlines* and *Register.com*, the courts, in determining whether there was "unauthorized access" (required by CFAA) considered the direct notice to both defendants that access was unauthorized. Southwest did so prior to suit, and, as the court noted in *Register.com*: "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."[128]

---

http://w2.eff.org/legal/cases/AA_v_Farechase/20030310_prelim_inj.pdf (last accessed Aug. 23, 2009)). I should note that, in this case, American Airlines would likely prevail under the self-help approach I advocate:

> Farechase's conduct has forced American to attempt self help. American time and resources have been dedicated to creating and implementing technological barriers in an attempt to block unauthorized users of Farechase software from accessing the AA.com computer system. Such actions by American to block have been circumvented by Farechase's intentional inclusion in its software of a "masking" feature by which the software disguises its identity so that American is unable to determine who is gaining access without authorization thereby preventing American from blocking all unauthorized access by the Farechase software.

Id. at 3.

124. In other words, trespass to land actions helped to create something akin to a land registry.

125. *See e.g.* Mark A. Lemley, *Place and Cyberspace*, 91 Cal. L. Rev. 521, 534 (2003) ("Even the staunchest advocates of propertization on the Internet tend to take for granted all sorts of public 'spaces' online . . . . [W]e rely on public 'space' on the Internet, just as we do in the physical world.").

126. *See e.g.* Epstein, *supra* n. 17, at 19 ("The ability of people to claim possession of particular things thus operates (by staking or branding, for example) as a way to give notice to the rest of the world that this patch of land or this animal has already been claimed.").

127. Note that these are requirements for property holders to be able to recover—akin to the affirmative burdens discussed above.

128. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000).

C. *Information Control and Copyright End Runs*

There is a danger that disputes over access to the system are merely subterfuge—what is truly at stake are "efforts to control the flow of information to or from a site."[129] The CFAA in fact goes quite far in the direction of "imposing limits on access and enhancing control by information providers."[130] Indeed, a "website provider can easily spell out explicitly what is forbidden" on its site.[131] Some courts have embraced a very wide definition of "unauthorized access to include unauthorized end uses of data obtained by legitimate access."[132]

At the extreme, the CFAA seems to have been pressed into service to create *de facto* intellectual property protection for subject matter that falls outside the purview of the intellectual property statutes.[133] There is a real concern that unqualified enforcement of trespass to chattels would in effect amount to a *sub rosa* intellectual property right in non-protectable subject matter. In effect, a party that could not secure copyright protection for data or information would nonetheless be given an enforceable right to control the information via the property rule protection of trespass law.

Content providers can achieve a substantial degree of control via self-help—technological measures as well as contractual arrangements. There is a risk that a trespass claim, especially one akin to trespass to land or trespass to chattels sans damage requirement, would go too far. Two high-profile cases illustrate this concern. In *Ticketmaster Corp. v. Tickets.Com, Inc.*, Tickets.com sent out web crawlers to Ticketmaster's website in order to get prices for events. Tickets.com was also deep-linking to Ticketmaster's website and displaying a small version of Ticketmaster's site in some frames. Ticketmaster brought a trespass to chattels claim. The court dismissed the claim, relying on the fact that there was no claim that the spider had dispossessed Ticketmaster of the chattel server.[134] The court, moreover, specifically rejected the

129. Lemley, *supra* n. 125, at 529. Lemley is part of a chorus of academics who would frame the issue as one of access to information, rather than access to a computer system. Such recharacterization, moreover, may be outcome determinative in the courts. *See e.g.* Dan Hunter, *Cyberspace as Place and the Tragedy of the Anticommons*, 91 Cal. L. Rev. 439 (2003).

130. *EF Cultural Travel B.V.*, 318 F.3d at 63 (rejecting the claim that "there is a 'presumption' of open access to Internet information").

131. *Id.*

132. *Register.com*, 126 F. Supp. 2d at 253 ("[E]ven if Verio's means of access to the . . . database would otherwise be authorized, that access would be rendered unauthorized *ab initio* by virtue of the fact that prior to entry Verio knows that the data obtained will be later used for an unauthorized purpose."). The court specifically rejected "Verio's distinctions between authorized access and an unauthorized end use of information" as "too fine." *Id. But see Intl. Assoc. of Machinists & Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005) (The CFAA does "not prohibit the unauthorized disclosure or use of information, but rather unauthorized access" and its terms do not "proscribe authorized access for unauthorized or illegitimate purposes.").

133. *See e.g.* 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, 323–24 (2004) (describing instances where the CFAA has been invoked to protect otherwise unprotectable information, such as non-copyrightable information, against unauthorized acquisition).

134. *Ticketmaster Corp.*, 2003 WL 21406289 at *3. The court does allow the contract claim to go forward. Ticketmaster has a detailed "terms of use" policy on its homepage. The detailed terms of use are not useful for providing tort liability, but they are the only method of self-help that provided for recovery in this case. *Id.* at *2.

notion that appropriation of Ticketmaster's data constituted damage; instead, the requisite damage had to be to the server itself. Nor was the court apologetic in dismissing the trespass to chattels claim: "[t]his approach to the tort of trespass to chattels should hurt no one's policy feelings; after all, what is being attempted is to apply a medieval common law concept in an entirely new situation which should be disposed of by modern law designed to protect intellectual property interests."[135] Here, the court gravitates to one pole—requiring actual physical damage to the server.

eBay v. Bidder's Edge represents the opposite pole. Bidder's Edge was scraping eBay's website and putting up price lists for items on eBay next to prices on other auction sites. In this case, the court credits eBay's trespass to chattels claim, with what comes close to an ode to Epstein's absolutist position:

> If eBay were a brick and mortar auction house with limited seating capacity, eBay would appear to be entitled to reserve those seats for potential bidders, to refuse entrance to individuals (or robots) with no intention of bidding on any of the items, and to seek preliminary injunctive relief against non-customer trespassers eBay was physically unable to exclude.[136]

In this case, eBay was primarily concerned about use of its price data. Bidder's Edge received information that could be accessed without submitting a username and password to eBay's website—in other words, it accessed what could be considered "public information." The auction listings would not be copyrightable and—unlike in the European Union—there is no special database right in the United States to cover them,[137] hence the creative resort to other theories. *eBay* has become the reigning example of use of trespass to chattels as an end run around copyright to sustain what is, in effect, anticompetitive conduct.[138]

Neither of these courts' positions, in the end, seems attractive, and the affirmative self-help requirement (as a substitute for the damages requirement) looks good by comparison. In those situations with the greatest danger that trespass to chattels and CFAA claims will be pressed into anticompetitive service or as an end run around copyright rules, the self-help requirements are apt to serve as a formidable barrier, in terms of having negative repercussions for the business model. For example, in the *Ticketmaster* context, there are technological self-help ways of making sure that webpages or images captured in frames are not displayed in external sites.[139] These do not seem to have been used, possibly because of negative business implications.[140]

---

135. *Id.* at *3.

136. *eBay, Inc.*, 100 F. Supp. 2d at 1067.

137. Guy Pessach, *Museums, Digitization and Copyright Law: Taking Stock and Looking Ahead*, 1 J. Intl. Media & Ent. L. 253, 276 (2007) (referring to "legal systems, such as the European Community, which recognize an independent sui generis database right") (citing Directive 96/9/EC of the European Parliament and of the Council of 11 March, 1996 on the Legal Protection of Databases (available at http://ec.europa.eu/archives/ISPO/infosoc/legreg/docs/969ec.html)).

138. *See e.g.* Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 Berkeley Tech. L.J. 561, 579 (2001); Maureen O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information?* 53 Vand. L. Rev. 1965, 1993–97 (2000).

139. It is possible, for example, to create webpages that check to make sure they are being displayed directly from the provider's machine.

140. Ticketmaster might have been able to program its pages so that any deep-linking or framed display

Likewise, self-help efforts could undermine eBay's business model. After all, eBay seeks to attract traffic to its site. eBay could remove price data from any users who are not logged in; use of this price data would then be covered under contract law according to the site's terms of use, but at the risk of losing customers.[141]

D. Technological Dimensions of Self-Help

Technological advances have the potential to assist as well as detract from the legal requirements of threshold self-help efforts.[142] The downside is that such a requirement could lead, as Epstein has forewarned, to a technology arms race[143]–a sophisticated version of the "cat-and-mouse game."[144] Such dire predictions may, however, be exaggerated,[145] and in any event, they could be mitigated by imposing reasonable limits on what amount of self-help is required. A separate concern (not raised by Epstein) is the temptation for actors to engage in "abusive self-help," or to take excessive measures in order to increase their potential damage award. Here, too, the dire scenarios seem overblown.[146]

---

would result in the user seeing a page stating that content used on Tickets.com's site was in violation of its terms of use. On the other hand, this might not be a good strategy: by the time a user has reached a framed page on Tickets.com's site, they are preparing to buy tickets and putting a hurdle in their way would be bad for business.

141. The case is complicated, however, given that eBay did exercise some modicum of self-help: it used robots.txt files to notify spiders of their exclusion policy—a policy that Bidder's Edge spiders simply ignored. *eBay, Inc.*, 100 F. Supp. 2d at 1061. *See supra* text accompanying nn. 50 & 61.

142. *Cf.* Douglas Lichtman, *How the Law Responds to Self-Help*, 1 J.L. Econ. & Policy. 215, 257 (2005) ("[T]echnology brings a new urgency to the question of how legal rules account for and respond to private self-help mechanisms."). Lichtman's article explores the ways in which legal rules encourage, harness, deter, and defer to self-help. He argues that technology creates new opportunities for self-help, for example, encryption to allow copyright holders to control work or Internet filters. Technology also expands the need for self-help because formal legal rules are often slow to respond to emerging technological threats. *Id.*

143. Richard A. Epstein, *Happiness and Revealed Preferences in Evolutionary Perspective*, 33 Vt. L. Rev. 559, 582 (2009) ("The current set of institutions and technologies has resulted in some kind of an arms race in which everyone is left exactly where they were before, at huge expenditures of wealth."); Epstein, *supra* n. 6, at 148 ("Today, each effort to place clever filters on email inspires new efforts by spammers to elude them in an endless arms war.").

144. Epstein, *supra* n. 6, at 151.

145. There is no evidence, for example, that Register and Verio engaged in the kind of cat-and-mouse technological self-help measures the court feared in *eBay*. Rather, everything seems to have centered upon cease and desist conversations between legal teams.

146. The specter of abuse was raised in *White Buffalo Ventures, LLC*, 420 F.3d 366, in which the plaintiff—a marketer of commercial services—brought a First Amendment action against a state university, which blocked the marketer's mass electronic mailings pursuant to its anti-solicitation policy, for violation of the marketer's commercial speech rights. In this case, the self-help measures—which included an email filter that blocked all email from White Buffalo Venture's IP address—were effective, which is why the plaintiff was suing a state actor to claim a violation of First Amendment rights. The self-help measures were effective because White Buffalo Ventures was sending spam admittedly compliant with the requirements of the CAN-SPAM Act. *Id.* at 371. This means that they were not fraudulent or deceptive and their origin was clear and identifiable. The plaintiff argued (albeit unsuccessfully) that because CAN-SPAM was meant to preempt any state laws regarding unsolicited bulk email, the anti-spam programs of UT's information technology department were preempted. *Id.* at 370–71. The court deemed "safeguarding the time and interests of those with UT email accounts" a substantial government interest, and thus rejected plaintiff's claim under the *Central Hudson* commercial speech test. *Id.* at 374 (citing *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Commn.*, 447 U.S. 557 (1980). The first prong of the *Central Hudson* test requires that the speech in question be truthful, non-misleading commercial speech that does not involve illegal activity. If that is the case, the court moves on to the next three requirements of the test. In order to be constitutional, the speech restriction must (1) be in

But there is an even more tempting—though often overlooked—upside to the legal inducement to engage in self-help. Self-help in digital—or, more broadly, nonphysical—arenas may on balance have net social benefits. Such innovative spillovers are less likely in the physical world, where self-help measures are more likely to be inefficient. Consider the land context, where self-help measures are more likely to be wasteful and duplicative and to divert resources from higher, better uses. Land is an old and familiar class of asset, not likely to be the forum for innovation. The same old moats, fences, etc. will be built by everyone. By contrast, with digital goods—more generally, with goods whose attributes are malleable or with goods with which society has little familiarity—self-help is more likely to lead to innovative spillovers. Different people have different ways of protecting their intangible goods; for example, Good X with self-help features Y may be a different good from Good X with self-help features Z.[147] Pursuit of these varied mechanisms of self-help, then, can lead to innovations that may be socially useful in other contexts.

CONCLUSION: EMBRACING THE ARISTOTELIAN GOLDEN MEAN IN DEFIANCE (AND IN HONOR) OF RICHARD EPSTEIN

Richard Epstein's take on cybertrespass dovetails with his longstanding war in favor of absolute private property rights; this is simply the latest battle. Epstein is well aware that twenty-first century courts have not signed on to his views here. Epstein's position was rejected in *Intel* and has likewise been rejected by most contemporary courts.[148] According to Epstein, courts' critical "misunderstanding [of the way in which a sound property system is organized] will invite courts to weaken the critical exclusivity requirement in favor of complex judicial schemes that decide which cases of exclusion are allowed and which are not."[149]

While Epstein's absolutist position has not (as of yet) captured judicial minds,

---

furtherance of a substantial governmental interest, (2) must directly advance the governmental interest asserted, and (3) must not be more extensive than is necessary to serve that interest.. *White Buffalo Ventures, LLC*, 420 F.3d at 374.

147. For example, an MP3 file with code that prevents the file from being ripped off is a different good from the same MP3 file with code that allows the file to be ripped off but causes the file to self-destruct after forty-eight hours. Consider the array of digital rights management (DRM) arrangements being layered into all sorts of consumer products. Whether one likes DRM or not, this is the start of a whole new field of innovation.

148. The one exception is *Southwest Airlines Co.*, 318 F. Supp. 2d 435, a case raising both trespass to chattels and CFAA claims. Farechase licensed software that was used by a third party to "access, search, and obtain data from Southwest.com by sending out a robot, spider, or other automated scraping device across the Internet" to allow "corporate travelers to search for airline fares." *Id.* at 437 (internal citations omitted). In other words, Farechase was spidering Southwest's website, which "provides proprietary fare, route, and schedule information to its actual and potential customers in an interactive format," in order to display pricing information. *Id.* The court upheld an injunction in Southwest's favor: "Because it is only seeking an injunction pursuant to its trespass claim, Southwest argues that it need not plead actual damage or deprivation of the use of the property for a substantial period of time. The Court agrees . . . ." *Id.* at 442. "In the instant case, Southwest argues that it has alleged enough to state a claim for trespass, although not enough to make Outtask liable for damages." *Id.* All this said, the court nonetheless apparently seems to think that Southwest may very well have had a claim for damages. The court finds that Southwest can meet the $5,000 threshold for its CFAA claim, reasoning that, while Southwest did not allege damages, it did allege "loss." (The court, however, is not clear whether this alleged loss was server time or other consequential damage.) *S.W. Airlines*, 318 F. Supp. at 443.

149. Epstein, *supra* n. 6, at 167.

Epstein has overlooked some history that could be mustered in support of his position. While the *Restatement* reflects the conventional understanding—as exemplified by Thomas Street's adamant position that harm to the chattel was an essential component of the trespass to chattels tort[150]—a contrary view nonetheless persisted at the time.[151] Frederick Pollock's position was "that in strict theory it must be a trespass to lay hands on another's chattel *whether damage follow or not.*"[152] Prosser and Keeton's torts treatise, moreover, cites a number of trespass to chattels cases from the nineteenth and early twentieth centuries in which actual harm to the chattel is not required.[153] Imagine Epstein's delight upon discovering yet another position of his aligning with a nineteenth century perspective on tort law!

Epstein stakes out resolute positions, often at the poles. He celebrates simplicity and clarity.[154] He eschews what he terms the "Aristotelian golden mean"—that compromise, middle-of-the-road position that seems the essence of reasonableness, but, under scrutiny, inevitably reveals itself as muddled territory betwixt two more principled extremes. In his words, "sound legal systems cluster closer to hard and fast rules than to the mushy middle gray ground."[155] And, he practices what he preaches.

In his seminal early work, Epstein railed against Aristotelian moderation, which he finds at the core of Judge Richard Posner's defense (or celebration) of the negligence standard in tort law.[156] The tempting "sounds of sweet reasonableness" are alluring, to be sure, but should be resisted:

> Moderation, Aristotle assures us, is a cardinal virtue that allows individuals to organize their lives for happiness and self-sufficiency . . . . Yet it is far from clear that Aristotle's steady middle-course plan . . . supplies an accurate guide to the soundness of academic or

150. Thomas Atkins Street, *Foundations of Legal Liability: Theory and Principles of Tort* vol. 1, 16 (Edward Thompson Co. 1906) ("It must be noted as important in connection with trespasses upon personal property that no cause of action arises unless the trespass is followed by actual damage. The application of force by one man to the chattels of another is not *per se* unlawful. The act is merely done at the actor's risk, and if damage follows he is liable for it . . . . Actual damage is essential to the cause of action.").

151. A view, moreover, to which the intermediate appellate court in *Intel* was partial:

> A trespass to chattels is actionable *per se* without any proof of actual damage. Any unauthorized touching or moving of a chattel is actionable at the suit of the possessor of it, even though no harm ensues. So it is a trespass for a shop assistant to snatch a customer's handbag and detain it "for a few moments," or to erase a tape-recording, or to show a private letter to an unauthorized person.

114 Cal. Rptr. 2d 244, 249 (App. 3d Dist. 2001).

152. Street, *supra* n. 150, at 16 n. 5 (citing Frederick Pollock, *The Law of Torts: A Treatise on the Principles of Obligations Arising from Civil Wrongs in the Common Law* 334 (6th ed., Stevens & Sons 1901) (emphasis added).

153. Keeton et al., *supra* n. 2, at § 14, 85 n. 4, 85 n. 6 (citing *Parker v. Mise*, 27 Ala. 480, 483 (1855) (holding that "although there be in fact no sensible damage from the loss or injury of the property, or from an actual deprivation of its use, the owner is entitled to recover some damages")); *Guttner v. P. Stream Whaling Co.*, 96 F. 617, 620 (N.D. Cal. 1899) (stating that "[a]ny unlawful interference by one with the property of another, or with property in the rightful possession of another, is a trespass upon such property . . . . Thus it has been held that, when a horse is hitched where he has a right to be, it is a trespass upon the part of another to unhitch and remove him against the will of the owner to another position, however near.").

154. *See e.g.* Richard A. Epstein, *Simple Rules for a Complex World* (Harv. U. Press 1995).

155. Epstein, *supra* n. 17, at 16.

156. *See e.g.* Richard A. Epstein, *The Perils of Posnerian Pragmatism*, 71 U. Chi. L. Rev. 639, 648 (2004) ("[W]hile reasonableness is a laudable goal, it is not a workable starting point for the analysis of [tort] problems.").

> legal positions . . .[;] the ostensible security of the middle position may be an illusion. Some corner solution may, but need not, be preferable to a compromise position that has all the sounds of sweet reasonableness about it, but nonetheless fails to achieve a set of optimal social results.[157]

Epstein has offered an alternative world, heading back to basics, where the goal is "to break down the cases into subcategories . . . and to develop a set of presumptive liability rules that govern each class of cases."[158] Epstein strongly believes that "the optimal legal rules are invariant to social changes,"[159] and that, "[i]n general, where private property and competitive solutions work, we can stick with older legal principles."[160] In fact, he would go so far as to say that "[w]hat was good enough for the second century A.D. is also good enough for us. Indeed, the position still seems sound on such critical matters as the basis of tort liability and remoteness of damage."[161]

Epstein's admonitions should be taken seriously. But, perhaps, they should not be taken all the way. In this article, I have tackled one cutting-edge tort issue—trespass to chattels (or personal property) on the Internet—which illustrates two more generalizable propositions. The first is descriptive: Epstein gravitates to extreme, absolutist positions—steadfastly based upon core Epsteinian first principles—and consistently resists Aristotelian golden mean approaches. For cybertrespass, Epstein's answer is strong property rights, akin to land rights, enforceable absent any showing of damage to the personal property. Enforcing strong property rights against infringements by "strangers" is a core Epsteinian principle.[162] The second proposition is normative: sticking to absolutist principles can be misguided, particularly in contexts where hybrid property entitlements present themselves. Trespass to chattels is one such example, where self-help emerges as the key pointing in the direction of reshaping the trespass to chattels tort, while keeping it distinctive from trespass to land.

157. Richard A. Epstein, *Why is This Man a Moderate?* 94 Mich. L. Rev. 1758, 1758 (1996) (footnote omitted).

158. Epstein, *supra* n. 154, at 648.

159. Richard A. Epstein, *Before Cyberspace: Legal Transitions in Property Rights Regimes*, 73 Chi.-Kent L. Rev. 1137, 1138 (1998).

160. *Id.* at 1154.

161. *Id.* at 1138.

162. Richard A. Epstein, *A Common Lawyer Looks at Constitutional Interpretation*, 72 B.U. L. Rev. 699, 714 (1992) ("The normal protection afforded individuals against the entrance of strangers on their property serves important interests. It creates an exclusive zone in which each person can control his or her own destiny, and it is an important instrument for the protection of individual privacy, the right to be let alone.").