JOURNAL OF LAW, ECONOMICS & POLICY

VOLUME 1 WINTER 2005 NUMBER 1

CONTENTS

SYMPOSIUM—PROPERTY RIGHTS ON THE FRONTIER: THE ECONOMICS OF SELF-HELP AND SELF-DEFENSE IN CYBERSPACE

BOOK REVIEWS

INTRODUCTION

In the waning months of 2002, likely due to the boredom induced by preparing for exams, a small group of students at George Mason University School of Law formed the idea for a new journal, the *Journal of Law, Economics & Policy*. Our plan was to create a peer-reviewed journal of law and economics that was, nevertheless, student-run. The journal was to have no normative agenda other than the notion that economic analysis of law and policy is a good idea. Beyond that, the purpose of the journal was to give economically minded students at GMUSL an outlet for their interests, and to publish quality, readable works. To our knowledge, this had never been done before, and so presented a challenge sufficient to keep us from seeing the light of day until our graduations.

Almost three years later, the issue you now hold was published. The Journal would never have gotten past the planning stages if not for the unwavering support of former GMUSL Dean Mark F. Grady, to whom the journal will always be indebted. Special thanks also go to his successor, Dean Daniel Polsby, who graciously continued to support a project funded by his predecessor. Professor Francisco Parisi, the journal's faculty advisor, and Professor Ross Davies of *The Green Bag* fame also deserve recognition for their continued support and encouragement.

This first issue is comprised of articles presented at a symposium, entitled "Property Rights on the Frontier: The Economics of Self-Help and Self-Defense in Cyberspace," which was held at the law school on September 10, 2004. The symposium was co-sponsored by the Journal and the Critical Infrastructure Protection Project. The law firm of Squire, Sanders & Dempsey LLP also generously sponsored portions of the event and went so far as to fly out Adam Fox, a partner at their Los Angeles office, to deliver the luncheon address.

For the last three years, the Journal has been an important part of our lives. We earnestly hope that it will also become a part of the lives of academics, students, and practitioners who believe, as we do, in the relevance of the economic analysis of law.

The Editors
Arlington, VA
March 15, 2005

THE THEORY AND PRACTICE OF SELF-HELP

Richard A. Epstein[*]

INTRODUCTION

Every successful legal system depends on an integration of two key elements. The first of these involves the articulation of a coherent theory of substantive rights. That theory must be internally consistent in order to provide guides for human conduct. Its principles must also be intelligible so that they can be followed by the mass of ordinary individuals who are bound by the law and by the government officials that are sworn to uphold it. And, ideally, the chosen rules must on average work for the overall social benefit, lest they lead to uncertainty, poverty and strife.

The articulation of the right set of legal norms is, however, only the first stage in a two-part struggle for the creation and maintenance of a sound social order. Of equal, if not greater, importance is the murkier topic of remedial choice and institutional design. No set of social norms, however desirable, will succeed if its substantive commands are widely and systematically disregarded, which will happen unless they are accepted as legitimate (even if not ideal) by large segments of the population. Once a breakdown in law and order is perceived, then it is only a matter of time before social peace starts to unravel. Even if most individuals are what we should self-consciously call law-abiding, any large population is sure to contain a few outliers who are eager to take advantage of any perceived gaps within the social or legal system. Their unilateral decisions will in

---

* James Parker Hall Distinguished Service Professor of Law, The University of Chicago; Peter and Kirsten Bedford Senior Fellow, The Hoover Institution. I should state at the outset that portions of this paper veered off into a discussion of evolutionary psychology in which I can claim no special expertise, apart form long term interest. But I have relied on the work of others, most notably John Haidt, Leda Cosmides and John Tooby. Haidt, Cosmides and I were together in June 2004 as part of a working group at a Dahlem Conference organized by Gerd Gigenrenzer on Heuristics in the Law. I would like to thank them and all the other participants for pushing my thinking further down this path. The application of these models to the principles of self-help is my own invention, but is I think compatible with the central insights of evolutionary psychology even if they are in tension with much of rational choice theory. The tension is not necessary. For an example of criticism of behavioral economics from an evolutionary perspective, see Richard A. Posner, *Rational Choice, Behavioral Economics, and the Law*, 50 STAN. L. REV. 1551, 1561 (1998). I take up the same line in RICHARD A. EPSTEIN, SKEPTICISM AND FREEDOM: A MODERN CASE FOR CLASSICAL LIBERALISM ch. 8 (2003), dealing with such topics as sunk costs, endowment effects and precommitment strategies. My thanks also to the participants at the Universiy of Chicago Law School Work in Progress, for their insistent comments and criticisms. Thanks also to Alix Weisfeld, Universiy of Chicago Law School, class of 2007, for her expert research assistance.

turn embolden others to follow the same course. At some point, even those individuals who prefer to respect the rights of others will have no choice but to fend for themselves as the entire system unravels. The outliers will, if left unchecked, dictate the social agenda as others follow suit.

Unfortunately, sound legal institutions and legal remedies are not easy to create, either by gradual evolution or by conscious design. The most powerful reminder of this simple fact is that the dustbin of history is littered with nascent societies that failed because they could not master the problems of coordination and production so central to organized life. These failures are not confined to the grand question of political organization. Local institutional breakdowns can occur in dealing with specific topics within an ongoing legal regime. The question of social order, to which the issue of self-help proves critical, thus, arises in two guises, one large and one small: The large question goes to the fundamental issue of global order. The small question goes to the resolution of particular disputes once basic order has been established. In thinking about these questions, modern legalists are heavily influenced by the Austinian conception of the law as a set of commands issued by a sovereign that are then backed by the threat of force.[1] That definition has a commendable generality and works reasonably well to distinguish a system of laws from a system of moral suasion, at least in developed societies. It leads us to think about the kinds of remedies that the state normally applies for the violation of its commands: fines and imprisonment on the public side; damages, injunctions, and specific performance on the private side.

Any emphasis on state-administered remedies is seriously incomplete; however, for it overlooks one set of practices that is a *ubiquitous*, if underappreciated, feature of all legal systems, ancient and modern: namely, the heavy reliance societies place on the use of self-help to enforce legal commands. For these purposes, it is useful to begin with a simple definition of self-help to set out the overall framework for analysis: "'Self-help'...denotes legally permissible conduct that individuals undertake absent the compulsion of law and without the assistance of a government official in efforts to prevent or remedy a legal wrong."[2]

Here several features of this definition call for immediate attention. First, the definition speaks about "individuals" in the plural, even though

---

[1] J.L. AUSTIN, THE PROVINCE OF JURISPRUDENCE DETERMINED, (Library of Ideas ed., H.L.A. Hart ed. 1954). For famous commentary, see H.L.A. Hart, *Positivism and the Separation of Law and Morals*, 71 HARV. L. REV. 593 (1958), reprinted in H.L.A. HART, ESSAYS IN JURISPRUDENCE AND PHILOSOPHY 49–87 (1983); Lon Fuller, *Positivism and Fidelity to Law—A Reply to Professor Hart*, 71 HARV. L. REV. 630 (1958). For my views, see Richard A. Epstein, *The Not So Minimum Content of Natural Law*, OX. J. LEGAL STUD. (forthcoming 2005).

[2] Douglas Ivor Brandon et al., *SPECIAL PROJECT: Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845, 850 (1984) (hereinafter Vanderbilt Special Project), which contains an exhaustive analysis of all the relevant precedents, and an accurate summation of the standard rules.

the word self-help typically evokes images of unilateral behavior by a single individual acting alone. But nothing about the analysis of self-help precludes one or more persons from acting in support of any individual or group of individuals that is subject to a wrong. The "posse comitatus" of old represents a group effort to track down outlaws, or individuals who act outside the scope of the law.[3] Any individual can join the posse even if his own goods and property have not been threatened or harmed. The morality and legality of these third person efforts are tested by the same standards that are brought to bear in individual cases, such that whatever action one person may do on his own, his friends and compatriots may do on his behalf. The use of cooperative activities for self-help raises the stakes, for it is easy for the posse in one case to become a band of marauders in the next.

Second, the words "legally permissible" are incautiously broad. This definition includes within the definition of self-help all sorts of simple devices used to forestall anticipated harm. Walking with friends on a well-lighted street is not only a way to get from one place to another, but it is also a way to prevent robbery, a legal wrong. People routinely lock the doors to their houses; remove valuable objects from plain view; sew name-tapes into garments; brand cattle; erect fences; and hire bodyguards. Instances of self-help, so defined, are socially ubiquitous. It is almost inconceivable to think of how any ordinary regime would treat these forms of assistance as illegal.

The question of self-help, however, becomes considerably more difficult when the user of self-help claims a "privilege" to use self-help. Here the term privilege is used in the sense found in the Restatement of Torts,[4] which is that special circumstances justify the commission of some act that constitutes a prima facie wrong, typically involving the use of force. In line with the definition of self-help, these coercive self-help remedies could occur before or after the occurrence of some wrongful act, that is, to either prevent a wrong from occurring or to remedy it once it has occurred. Illustrations of these narrower self-help rules deal with self-defense, the defense of property, the recapture of land or chattels, or the abatement of a nuisance.[5] Self-help in this sense also covers various cases of citizen's arrest, and it extends to the rejection of goods under a contract, which one is prima facie obliged to accept. Since these instances of self-help are themselves

---

[3] A group of citizens who are called together to assist the sheriff in keeping the peace. BLACK'S LAW DICTIONARY 1183 (7th ed. 2001).

[4] §10: 1) The word "privilege" is used throughout the Restatement of this Subject (Intentional Harms to Persons, Land, and Chattels) to denote the fact that conduct which, under ordinary circumstances, would subject the actor to liability, under particular circumstances does not subject him to such liability. 2) A privilege may be based upon a) the consent of the other affected by the actor's conduct, or b) the fact that its exercise is necessary for the protection of some interest of the actor or of the public which is of such importance as to justify the harm caused or threatened by its exercise, or c) the fact that the actor is performing a function for the proper performance of which freedom of action is essential.

[5] *See* 3 WILLIAM BLACKSTONE, COMMENTARIES § 2-5 (1769).

presumptive wrongs, the circumstances that privilege them are often sharply circumscribed in ways that ordinary means of self-help are not. People can stay home as much as they like to avoid harm in public places. But they cannot bring unlimited force to forestall or remedy those harms.

Any complete analysis of the problem requires, therefore, an understanding not only of the uses and limitations of each of these self-help remedies, but also their interaction with state-supplied remedies administered by public officials. Outlining the proper interplay between self-help and legally administered remedies is one of the primary objectives of this article. In order to approach this problem, this article proceeds in stages. The first section deals with the question of self-help in a state of nature, offering both an account of human nature, moral responses, and a close examination of the legal rules used in this context. The great challenge here, which sets the stage for all that follows, is to explain why a pure system of self-help that characterizes a society in the state of nature has at least a fighting chance to succeed, or at least to stay above water. The bottom line is that self-help would be doomed to failure if the Hobbesian vision of unbridled egoism held firm; but precisely because that model is profoundly wrong, self-help allows some primitive societies to succeed on a modest scale.

The second section examines the transition from a state of nature into civil society, with an analysis of why self-help remedies continue to hold an important place in the overall legal system in ancient and modern societies. Legal enforcement expands the array of useful options. But the key insight remains: the basic rules of primary conduct (i.e., those that arose naturally to regulate conduct between ordinary individuals without interference from the law) that arose in a regime of pure self-help offer the best structure for individual rights and duties *even after* the creation of a viable public force.

I. SELF-HELP IN A STATE OF NATURE

Let us start with the question of whether we can conceive of a regime of pure self-help that functions in a state of nature, that is, in a society that does not have any sovereign to maintain order or to resolve individual disputes. In a brute historical sense the answer to that question has to be yes. Although it is commonplace in modern discourse to write as if property rights—and, less frequently, rights of personal autonomy—are solely the creation of the state, historically, the evolution runs in the opposite direction. All sorts of familial and communal organizations operated prior to the emergence of the modern nation (or even city) state with systems of centralized governance endowed with monopoly power over a given territory, whose inhabitants are not all blood relatives with each other. Jared Diamond notes that, in order of increasing size and complexity, these governing organizations include bands (with a population of about 5 to 80 members), tribes (in the hundreds), chiefdoms (in the thousands), and then the

modern territorial state (which he defines as having over 50,000 people).[6] Only the modern state has a full blown judicial system separate and apart from other aspects of governance. In contrast, the earlier nomadic organizations, especially the small bands, might well have failed more often than they succeeded. They could be brought down by drought, flood, frost, disease, conquest, or by just plain bad luck. Nevertheless, those groups that did succeed had to generate enough resources to allow them to maintain the basic necessities of life and to ward off their enemies, who faced similar organizational difficulties.

The key theoretical questions for political thought are two: First, what types of human attributes dominate those primitive groups that eked out a hardscrabble existence without the benefit of central government? Second, to what kind of rules did they instinctively resort in order to achieve that end? Let us take them in order.

A. *Dominant Attributes Among Members of Primitive Societies*

One basic model of human behavior posits that all individuals act with a relentless form of self-interest, such that their own utility functions do not take into account either the benefits or costs of their actions to any other individuals. All they care about is their own welfare, so that the smallest private gain is sought no matter how great the harms caused to others. Thomas Hobbes has penned an extreme and compelling version of this all-consuming vision. He paints a portrait of human beings in the state of nature that is so grim—"worst of all continual fear, and danger of violent death; and the condition of man, solitary, poor, nasty, brutish and short"[7]—that "rational" individuals will do just about anything to escape from that condition, including accepting by covenant any arrangement that binds them to the absolute whims of a sovereign whose chief ability is to prevent an individual from engaging in acts of depredation against another.

The great appeal of the Hobbesian model is not its historical or biological realism, for of that it has none. Rather, its appeal comes from the challenge that it throws up to political theory. If we can find a way in which ordinary individuals with these characteristics can surmount their differences, then surely it is far easier to account for political power within the state on weaker assumptions that attribute even a grain of conscience, empathy, or benevolence to ordinary human beings. The genius of Hobbes is that he probes the strengths of this model in ways that show—conclusively—the difficulty of social organization for individuals consumed by such single-minded ends. In the state of nature, cooperation over

---

[6] See JARED DIAMOND, GUNS, GERMS AND STEEL 268-269 (1997), for the table. Note that all large states have centralized institutions, not based on kin, for resolving disputes.

[7] THOMAS HOBBES, LEVIATHAN, ch. 13. (1651).

time becomes a nonstarter because of the overpowering risk of defection. For example, assume there is a deal from which both A and B will benefit, but in which performance is sequential: A must perform before B. The object of an agreement is to assure A that he can expect the return performance, which will induce him to go first. If universal defection is the norm, then A will not perform first because he is confident that B will not perform when his time comes. The entire process of cooperation will grind to a halt without someone to watch over us. Yet, in a state of nature that distinctive sovereign, under Hobbes's strongly individualistic assumptions, is just not there.

The Hobbesian mission was to prove that the gains from social organization are so great that even the most hardened individuals would prefer to yield unquestioned power to a sovereign than to run the risks of constant defection in the state of nature. But this stark model suffers from two incurable weaknesses. First, it cannot explain how individuals in a state of nature initially acquire enough wherewithal to survive long enough to decide whether to sacrifice their natural liberty for the legal protection of a sovereign, whose own effectiveness must be open to question, given the enormity of the challenge he faces. Second, it does not explain how any system could in fact provide that protection if all individuals, both governed and governors, were dominated by these relentless passions to look out always and exclusively for number one. Defection today, rationalization tomorrow becomes the dominant mode. Let individuals lie, betray, attack and scheme, and no one could form any voluntary association even for such modest tasks as hunting or farming. Marriage would become an impossibility. It strains credulity to believe, therefore, that these same individuals could in large numbers come together in any real world—that is, territorial—setting for the more ambitious task of putting a government over their heads. We should expect to see, at most, tiny clots of individuals huddled together under the crudest of circumstances, forever watching their backs. The productive division of labor and voluntary exchange would be dead on arrival, and with them any form of social order or of human progress.

Any descriptive account of how a regime of self-help operates in the state of nature must relax the Hobbesian assumption of relentless self-interest. The question is what sort of adjustments should then be made. Here it is critical to avoid lurching toward the opposite extreme that postulates that individuals who are short on food, clothing and shelter basked in a primitive form of socialism in which each contributed according to his ability to a common kitty from which each extracted resources from the social commons in accordance with his need. Systems of redistribution on such a broad scale would be highly vulnerable to the machinations of all self-interested persons. In an environment where every calorie counts, these naïve indulgences could not work out. Rather, the better working assumption holds that self-interest remains a powerful force and motivation for individual behavior, but is, decidedly, not the only one. Rather, in any real

world setting it is tempered by a rich set of emotions and intuitions that are subject to powerful evolutionary pressures.

B. *A Biological Predisposition Toward Cooperation*

At this juncture, key strands of the argument are drawn from the field of evolutionary psychology that follows up on the central Darwinian insight that the evolution of both cognition and emotions follows the dictates of natural selection, just as the obvious physical traits to which the doctrine unquestionably applies. Chance (here, mutation) throws up all sorts of individual traits, of which the fittest for any particular environment survive to be passed through to the next generation in greater proportion than their alternatives. Darwin's theory does not operate with an eye to advancing any modern ethical ideal of communal association; of course, its only currency for natural selection is that of the propagation of genes through the survival of individuals who bear them. However, the machinery of evolution could *never* have lead to the emergence of a stable population composed solely of Hobbesian individuals. Something besides self-interest has to be added to the mix for the system to work and for communities to flourish. What counts are those additional ingredients.

The initial inquiry is into the optimal division between inbred and learned traits. To the British empiricists, the class of "innate ideas" was empty. All was learned through experience.[8] That position is most certainly wrong, for it is now known that some capacities and traits are hard-wired, even if others are not. The mind is not a blank slate, but a complex organism that contains much innate information that is coupled with the capacity to acquire more. As John Tooby and Leda Cosmides have written of the modern behaviorist, B.F. Skinner: "Skinner's hypothesis—that learning is a simple process governed by reward and punishment—was simply wrong."[9]

The question is what principles determine the division between these two classes of knowledge. I think that the basic difference runs as follows: the lower the variance of certain phenomena in nature, the more likely that dispositions to respond to them will be hard-wired. The analysis depends on a simple consideration of error costs. In the extreme situation, where natural conditions are totally invariant, any organism that programs in ad-

---

[8] *See, e.g.*, JOHN LOCKE, AN ESSAY CONCERNING HUMAN UNDERSTANDING ch. 2. See also, chapter 9, arguing that the ostensible innate responses of children just reflect what they have learned through sensation while in the womb. For a summary of evidence on how baby's minds are wired see STEVEN PINKER, HOW THE MIND WORKS 316-321 (1997). See also, for a general critique of the Lockean position, STEVEN PINKER, THE BLANK SLATE (2002)

[9] Leda Cosmides & John Tooby, *Knowing Thyself: The Evolutionary Psychology of Moral Reasoning and Moral Sentiments*, 4 BUS., SCI. & ETHICS 91, 94 (2004).

vance the proper response to those conditions will have an enormous survival advantage over rivals who have to acquire that information on the fly. The quick and automatic responses to external stimuli reduce the possibility of error—and death. It also frees the discretionary powers of perception and intellect to respond to specific challenges that do vary by time and place. Over time, strong selection pressures will lead these responses to be hard-wired in the brain.

The most obvious candidates for invariant status are the laws of physics, which explains the innate ability to deal with space and time, which Kant singled out as part of the synthetic a priori (i.e., nonlogical judgments that are made before experience is acquired).[10] These capacities need not be fully functional at birth but may be programmed to manifest themselves at some critical point in the life cycle. Similar arguments explain other invariant features of our natural environment: the connectivity of objects, the differences in color and shape, and the like. No newborn has to learn to operate these categories from scratch, for they run (to borrow a phrase from the computer age) in the "background" even while the conscious mind is actively engaged in other activities.[11]

In addition to developing an innate fight or flight response, another key response is an altruistic one. Although in many cases operating in less acute situations, it is by no means less significant: humans need other humans to survive, beginning with the family.[12] Close association of a newborn with its mother, and perhaps both its parents, is invariant because offspring cannot hope to survive without protection, nourishment and support; the parents cannot hope to propagate their line unless they take care of their offspring until maturity. Parents and offspring alike have an enormous incentive to cooperate over a broad range of activities, even if their interests tend to diverge as their offspring get older.[13] It is, therefore, no curiosity or accident that the first impulse in the young is not to think of spot exchanges, but to grasp some ideal of communal sharing that extends beyond the mother to other siblings.[14] Indeed, as the relationship evolves, the offspring also work for the benefit of the larger unit, including other siblings. Other instincts follow. An awareness of harm, from which springs tort.

---

[10] For an elaboration of this theme, see Gerd Gigerenzer & Klaus Fiedler, *Minds In Environments: The Potential of an Ecological Approach to Cognition*, (on file with author).

[11] PINKER, HOW THE MIND WORKS, *supra* note 8 (denoting the various tests for objects. All these break down at the margins. Query: is a newspaper one object, or a collection of several individual sheets? Does it depend on whether they move in unison, or as separate sheets?)

[12] For a discussion on which I have heavily relied, see Jonathan Haidt, *The Emotional Dog and Its Rational Tail: A Social Intuitionist Approach to Moral Judgment*, 108 PSYCH. REV. (2001).

[13] To be sure, conflicts of interest between parent and offspring do arise farther down the road, but simply because the offspring wishes to receive more intensive care for longer than the parent wishes to supply it. *See* Robert L. Trivers, *Parent-Offspring Conflict*, 14 AM. ZOOLOGIST, 249 (1974). *See also* Robert L. Trivers, *The Evolution of Reciprocal Altruism*, 46 Q. REV. BIOL. 35 (1971).

[14] *See* PAUL H. RUBIN, DARWINIAN POLITICS: THE EVOLUTIONARY ORIGIN OF FREEDOM (2002).

There are also cooperative responses to avoid harm that undergird the implicit norm of reciprocity. This norm becomes closely associated with the idea of contract, and of course its doctrine of consideration that lies at the root of sale, hire, partnership, lease, loan, and the like. These forces necessarily falsify the strong Hobbesian account of *individual* self-interest in familial relations to which Hobbes (unlike Locke[15]) gives no attention.

In stranger cases, however, the genetic overlap is negligible, so the dominant motif among conspecifics is universal separation followed by selective cooperation, in that order. Keep off, go one's separate ways. It takes little imagination to understand that once someone violates your person by crossing into your space, he deprives you of the resources needed for survival. Children internalize the norm against hitting other children (if they do not universally follow it) with little or no instruction at a very early age. Even those children who attack others know it is wrong. The stakes are too high for learning to be postponed to the age of conscious understanding.[16] But any basic rule of territory or property that protects exclusive possession does not necessarily insure gains from trade. Hence, we find a natural progression that starts with family status and extends to successively larger units. The more extensive the social unit, the more likely it is that traditional principles of property, tort and contract operate as minimum conditions for any form of social life. The informal adjustments among intimates are replaced by clear boundaries with strangers.

All of these different types of rules for various interactions require a unique remedy. In primitive societies, of course, these were necessarily self-help remedies. The missing piece that helps explains the *partial* success of human self-help mechanisms is the reflex-like speed and reliability in which people apply these basic norms to discrete cases. On matters of perception, intuition tends to beat rationalization hands down. Our ability to organize sense data into recognizable patterns takes place in an effortless and nonreflective manner, or as is often said in a "fast and frugal" way.[17] This heuristic allows us to act before opportunities slip away or before we have time to form a rational plan to deal with impending dangers. In nature, there is not the luxury to pose the Kantian question of whether one's actions satisfy the rigorous demands of the categorical imperative. Put otherwise, the question of moral judgments must satisfy in any self-help situation the same requirements for fast and frugal decision-making that control in perceptual areas. Individuals make their quick intuitive judgments first and then develop explanations as to why these are correct only after the fact,

---

[15] *See* JOHN LOCKE, SECOND TREATISE OF GOVERNMENT 42-52 (1690) ("Of Paternal Power," which speaks of parental power in some detail.).

[16] Haidt, *supra* note 12, at 822-823.

[17] Gerd Gigerenzer & Daniel G. Goldstein, *Reasoning the Fast and Frugal Way: Models of Bounded Rationality*, 103 PSYCHOL. REV. 650 (1996).

often in the effort to justify their conduct to others.[18] No one has, as with learning a musical instrument, the option of continual practice until playing, as it were, becomes a matter of "second nature."

It is, therefore, critical to ask what kinds of predispositions will make those rapid-fire judgments work. That requires a conjunction of two conditions: there has to be some moral sense or sentiment, of the type emphasized by such writers as Hume and Smith,[19] in favor of cooperation. And the rules in question must be clear enough so that all parties—both participants and observer—are able to tell who is in the wrong, so that one party to the dispute will be likely to back off from a confrontation that could prove fatal to both. This moral sense does not violate the standard evolutionary norm of natural selection, for a strong moral sense could aid those who possess it. Entering into any sort of conflict is often costly even to the *victor.* Those who are injured in the first round will be much more vulnerable to attack in the next round,[20] which is why fair fights are not found often in nature. To be sure, cooperation may not look like a sensible evolutionary strategy if one thinks about an isolated two-party squabble. But it becomes a much more plausible strategy in any realistic setting in which multiple individuals have to decide whether to trade, cooperate, ignore, or attack others over many periods, where new rivals and allies are always waiting in the wings.

Interestingly, it takes only a "small" change in personality to execute this seismic shift.[21] The usual version of the prisoner's dilemma game indicates that a single party (in a nonrepeat situation) is better off if he defects no matter what the other side does. But if it is tacitly known that there is some genetic predisposition to cooperate, then the balance of advantage shifts. Anyone who is prepared to go first to induce cooperation from others will now know of a positive probability that others will reciprocate given their own set of genetic endowments. Now if the probability of success is high enough (and if the amount placed at risk in the initial period is low enough), then reciprocation will follow. If one good deed deserves and begets another, then each party will cooperate at each stage in order to preserve the gains from a long-term relationship, with an optimal social result.[22] That pattern of sequential cooperation in turn yields a vastly superior

---

18 Haidt, *supra* note 12, at 814.

19 *See* DAVID HUME, A TREATISE OF HUMAN NATURE (L.A. Selby-Bigge ed., 1888) (1739-1740); ADAM SMITH, A THEORY OF MORAL SENTIMENTS (1759); and for a modern version of the theory see JAMES Q. WILSON, THE MORAL SENSE (1993).

20 For discussion of the sequential element see Richard A. Epstein, *A Taste for Privacy: The Evolution of a Naturalistic Ethic*, 9 J. LEGAL STUDIES 665 (1980).

21 *See* Robert Axelrod and William D. Hamilton, *The Evolution of Cooperation*, 211 SCIENCE 1390 (1981).

22 Benjamin Klein, *Self-Enforcing Contracts*, 141 J. INSTITUTIONAL & THEORETICAL ECONOMICS, 594 (1985); *see also* Benjamin Klein, Robert G. Crawford, & Armen A. Alchian, *Vertical Integration, Appropriable Rents, and the Competitive Contracting Process*, 21 J.L. & ECON. 297 (1978).

social outcome to a universal decision to defect, which reinforces total social isolation. The impulse to share in hard times counts for much more than in regimes of relative prosperity. If I have 10 and you have 2, and 5 are needed for survival, then a 6 to 6 split has real power, which is one reason why the traditional references to redistribution always dealt with cases, as Locke put it, of "extreme want."[23] But if I have 100 and you have 20, with survival still pitched at 5, then the gains from equal distribution are far smaller. The path toward cooperation is eased between siblings with genetic overlap, selfish genes notwithstanding.[24]

Cooperation may be learned in infancy when parents (the localized sovereigns, as it were) are present to moderate disputes, but it is hardly confined to those situations. Sibs will continue to interact after the death of their parents.[25] It is, in this regard, telling that the origin of the commercial partnership is in all likelihood tied to continued cooperation between siblings after the death of the parent when each of them, at least in Roman law, first assumed the status of independent persons.[26] From there it is easy to imagine various extensions of the basic program. The new partners (for either a particular venture or on some more permanent concern) could be distant relatives (e.g., first cousins); or there could be a mixture of children and cousins, mixed with outsiders. On these issues, evolution is not a precise instrument. The errors of *not* cooperating within families are very costly, so that a pattern that extends cooperation to chosen outsiders (friends, as it were) could well prove to be far more favorable than hostility or aloofness. The instinct for cooperation within families will by degrees extend beyond it.

Some powerful evidence that supports the position that limited forms of cooperation exist is—what Hume perceptively called "confin'd generosity"[27]—the social norm. One simple point is that individuals engage in moral discourse about the conduct of third persons and, through literature and art, hypothetical situations, even if there is no direct feedback to their

---

23 JOHN LOCKE, TWO TREATISES OF GOVERNMENT 188 (Peter Laslett ed., Cambridge Univ. Press 1988) (1690) ("Charity gives every man a title to so much out of another's plenty, as will keep him from extreme want...").

24 RICHARD DAWKINS, THE SELFISH GENE (1990).

25 This point is one feature that is missing in Gary Becker's work that posits that parents have an interdependent utility function with their children, even if children do not have it with each other. On that assumption, the children should become strangers after the parents' death. The Becker model works much better in international settings where one nation may decide to play power broker between two others who are not bound by any natural ties. Nations do not die, even if they will occasionally falter, so that these arrangements could prove tolerably stable in at least some settings. Gary S. Becker, *A Theory of Social Interaction*, 86 J. OF POL. ECON. 1063, 1076-83 n.6 (1974).

26 *See* GAIUS, THE INSTITUTES OF GAIUS PART I 203 §154(a)-(b) (Francis de ZuLueta trans., Oxford University Press 1945) (c. 140 AD).

27 DAVID HUME, A TREATISE OF HUMAN NATURE at 495 §2, ¶ 18 (L.A. SelbyBigge ed., Oxford University Press 2d ed. 1978) (1739-40).

own lives. Stated crudely, people love to gossip.[28] This behavior is self-interested in an extended sense, however, because it allows people to reinforce the applicable social norms while applying them to concrete cases. The intrinsic pleasure from the discussion appears sufficient to overcome any familiar free-riding objection. Nor should we ignore the indirect benefits of such behavior; it helps develop the ability to organize and align cases that permit people to make moral judgments when their own welfare is directly on the line. The use of these techniques works to defeat claims of moral relativism in practice.[29] To the charge that you didn't keep your promise, you can't blithely respond that promises just don't matter. What you have to do is give some more particularistic explanation as to why this specific charge is ill-founded. It could be that the promise was never made, that it had a content different from that alleged, or that it was defeated by duress. The point here is that once people start to talk this way, they have conceded the force of the basic moral premise about promising as a social institution as the price for admission into society. Ordinary language has moral force, which is why the economic jargon (of which I am a fierce devotee) often falls on deaf ears in standard moral discourse, even when that language *reinforces* the moral intuitions of ordinary people.[30]

The pool of strong collective moral sentiments has its own behavioral consequences, which serve to reinforce the tension between the approach of evolutionary psychology on the one hand and rational choice economics on the other. One simple observational trait is that it seems clear that individuals will act at their own risk in order to enforce the moral norms of the basic society. The rational choice model posits that individuals will happily take on the role of moral free riders in the face of asocial conduct, which includes everything from bullying to littering or worse, that threatens large numbers of individuals. The argument is that the individual actor has to bear the entire cost of its intervention but receives only a fraction of the benefits. We thus have the standard dilemma of collective action which is: private benefits are less than private costs which in turn are less than social benefits.[31] The rational individual actor compares the first two terms; but

---

[28] Haidt, *supra* note 12, at 826.

[29] For a neat discussion of how this works see C.S. LEWIS, THE CASE FOR CHRISTIANITY §3 (1943) (the point, of course, can be used in defense of any form of standard moral discourse.); *see also* RICHARD A. EPSTEIN, SKEPTICISM AND FREEDOM: A MODERN CASE FOR CLASSICAL LIBERALISM 84 (2003) (applying the logic to standard legal reasoning and seeking to bridge the gap between ordinary discourse and more academic consequentialist reasoning).

[30] Here is one true anecdote about the difficulties of persuading ordinary people to use economic language: Years ago at a Liberty Fund Conference, I was talking on about some problem, using some standard economic jargon. An English professor, whose name I forget, from Wofford College in Spartanburg, South Carolina said that he did not wish to take an exception to anything I had said, but thought that he could run a tape of my little speech and have me civilly committed in any state in the union.

[31] *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1965) (the standard reference on this point).

socially we would like him to compare the last two terms (at least on the assumption that he his private costs are equal to social costs). The bottom line is that various coercive devices, e.g., taxes, are needed to align individual with social incentives. The common observation, however, is that some people will act to defend social norms even when costly or risky to do so. Their own levels of participation are strong determinants of their willingness to enforce the collective norm, even if others benefit from that action. Indeed, it appears that people care about raising their own level of participation more than any direct benefit they receive from their own intervention.[32] These findings deviate from those of rational choice theory, which postulates that people will only punish free riders when it is in their narrow personal interest to do so.[33]

The evolutionary models thus give an account of ordinary sociability that hold out greater prospects for general cooperation and sociability to the strongly individualistic Hobbesian theory. A second way to make the same point recounts what happens to those few individuals whose emotional deficits make empathy and cooperation impossible. Those individuals who have no consideration for the suffering of other individuals are termed psychopaths precisely because their reasoning and judgment about individual cases is radically dissociated from any emotional or empathetic component.[34] The behaviors in question are not just small variations in some normal distribution; they are discontinuous differences from the usual gradations in ordinary sensibilities about other individuals. They are similar in nature and kind to the radical separation of reason and emotion that Damasio has reported with respect to individuals who have received serious brain damage in the ventromedial area of the prefrontal cortex.[35]

Yet another instance of the gap between emotion and cognition occurs in autistic individuals. One standard puzzle in the philosophy of mind is the problem of "other minds," that is, whether any one person can infer from the outward behaviors of other individuals whether they have minds or are merely some form of automatons. The narrower question is if we concede that there are other minds, how do we know what they are thinking? Most ordinary people scoff at these matters. They may agree that X has a poker face on this or that occasion, but they cannot conceive of a world in which they are barred from accurate mental knowledge of other people's states. Indeed, frequently, as in courtship and recruitment, the whole point is to make clear the positive state of mind that one person has to another. In many contexts, it is the concealment of mental states that strikes us as odd.

---

32 Cosmides & Tooby, *supra* note 9, at 108-09.

33 *See id.* at 111. (See Table 1 for a compilation of the differences.)

34 Haidt, *supra* note 12, at 824 (discussing Hervey Cleckley, *The Mask of Sanity* (1955)).

35 *See id.* at 824 (discussing Antonio Demasio, *Descartes' Error: Emotion, Reason, and the Human Brain* (1994)).

The legal response to the question of other minds arises constantly with the question of mens rea in criminal law, and with intent facts in virtually all areas of private law. The law on this question is much closer to the robust views of common sense because it assumes that ordinarily external acts are strong evidence of internal mental states: actio exteriora indicant secreta interiora—external acts indicate internal secrets. The most famous bon mot in this regard is from Bowen, L.J., in a fraud case, that "the state of a man's mind is as much a fact as the state of his digestion."[36] In fact most individuals can tell something about mental states, and develop some ability to detect cheaters, with whom it is so costly to deal.[37] Thus, one group of individuals who are incapable of drawing inferences about mental states from observed action is autistic children.[38] For most individuals, the inference from behavior to intention is so easy to grasp that it prompts no account or judgment at all, precisely because ordinary people develop the skill to read faces.

The basic truth is that the full range of emotional equipment moderates strongly against the Hobbesian model, and allows for the emergence of some level of cooperation in a state of nature. No one should draw the conclusion that these mechanisms work in a fail-safe manner. After all, if most individuals find it in their biological self-interest to read emotions and to detect cheaters, at least some individuals stand to gain if they hone their skills at dissimulation and deception in order to continue with their devious ways. There is no way in which human beings can avoid this particular "arms race" between those who get ever more skillful in cheating and those who become ever more sophisticated in ferreting it out. In effect, therefore, there will be something of a competition between individuals with the two different forms of character, where it is not clear which one will win out in any particular case. But this centralizing tendency does seem clear. If high levels of egoism and emotional dissociation had prevailed, then we should not have been born to tell the tale. The basic pattern is that *most* individuals converge on some moral norm, so that in equilibrium any successful society

---

[36] Edgington v. Fitzmaurice, 29 Ch. D. 459 (1885); *cf.* Y.B. 17 Edw. 4, f. 2, Pasch pl. 2 (1486) (The most famous statement of the other side is from Brian, C.J. "The thought of man shall not be tried, for the devil himself knoweth not the thought of man." But this quotation was made in a very different context, namely, on the question of whether a person in a contract could be bound by an unstated term or condition. The point of this rule is to be sure that people do not escape from legal obligations by positing undisclosed conditions. So, in the former context, it is correct to be hostile to evidence about mental states, but that same attitude has never been carried over to fraud cases, where it would gut all legal protection.)

[37] Cosmides & Tooby, *supra* note 9, at 99-103 ("Perhaps the strongest evidence that there is a neural specialization designed for cheater detection is the discovery that cheater detection can be selectively impaired by brain damage, without impairing other reasoning abilities."); *see also*, PINKER, *supra* note 11 at 336-37, 403-05.

[38] Cosmides & Tooby, *supra* note 9, at 97 (discussing Simon Baron-Cohen, Mindblindness: An essay on Autism and Theory of Mind (1995)); *See also* PINKER, *supra* note 11, at 329-333.

is able to deal with the few outliers in a manner that reduces their corrosive effect on everyone else. Yet there are no guarantees here. The same theory that postulates the possibility that some groups will be able to confront the risks of egoism also shows that when the forces align the wrong way, these forces can be overwhelmed by greed, avarice and aggression. The same is true in international relations, where the realist account of relentless self-interest is often false to the facts: voluntary compliance borne of a latent sense of sociability is as much a part of that tradition as acts of treachery and betrayal.[39] And in both contexts, the tipping point, moreover, is often unstable and, to make matters worse, often unknown.

C. *Making Self-Help Remedies the Rules of the Game*

The purpose of this apparent digression is to show that it is not idleness to speak of a viable regime of self-help in a state of nature. Stated otherwise, the Lockean view that most individuals behave well most of the time in a state of nature, and that the true difficulty is responding to outliers (as well as external aggression) has more truth than any alternative account that makes relentless self-interest, shorn of empathy, the universal behavioral pattern. But this set of behavioral insights is not sufficient to explain how self-help regimes emerge in a state of nature. A good deal of attention has to be given to the particular rules that comprise this legal regime. In this context, self-help remedies all go to the core libertarian concerns with the use of force. (Even fraud, standing alone, is not the key issue, because the first line of self-help defense is a suspicious mind.) The areas involve such matters as arrest, abatement of nuisance, eviction of tenants, self-defense, defense of property, privileges of necessity and the like.

In dealing with these elements, the constant stress is one for simple rules. Quite foreign to the debate is that outgrowth of administrative law, with its enormous and inconclusive debate over the relative advantages of rules and standards in running the modern bureaucratic, or cost-benefit, state.[40] The pure version of a standard involves the articulation of some basic social objective, often expressed at a high level of generality, which then invites the creation of a list of relevant considerations of indeterminate weight, all of which must be reviewed before some administrative decision is made. Here it is easy to multiply examples. The modern tort law has tests for liability that depend on whether a particular product is reasonably

---

[39] For a discussion of the "expressive" theory of human nature, which is said to account for this result, see Tom Ginsburg & Richard H. McAdams, *Adjudicating in Anarchy: An Expressive Theory of International Dispute Resolution*, 45 WM. & MARY L. REV. 1229 (2004) (noting the complex elements that allow stable equilibria to emerge in some international law settings, with state of nature overtones).

[40] *See* Matthew Adler & Eric Posner, *Cost-Benefit Analysis: Legal, Economic and Philosophical Perspectives*, 29 J. LEGAL STUD. 837 (2000).

safe, which in turn rests on a multitude of factors dealing with the anticipated risks and the various techniques used to counteract them.[41] The 1996 Telecommunications Act contains an exhaustive checklist to determine whether local exchange carriers are allowed to enter long-distance phone markets from their home base.[42]

None of this institutional refinement is remotely conceivable in the state of nature.[43] Rather, the practice lurches sharply in the other direction toward rules that in their simplest form operate as litmus tests. There are only two states of the world, and a different up or down decision applies to each state. Thus, an extreme version of a rule is one that says if you cross this boundary line, you are guilty of a trespass: the question is no more complicated than deciding whether a baseball has landed fair or foul. Even the simplest legal rules that focus on clear boundaries and boundary crossings will not be able to maintain accuracy at a 100 percent level. Any on/off switch can fail. The ball which leaves the stadium far above the foul pole (which is itself installed to ease the perceptual burdens) is but one example of the low-probability dangers that are inherent in all systems.

In addition, there is a larger class of issues that can not be dealt with so easily. As the definition of self-help outlined above suggests, there are always cases where crossing a boundary line turns out, as in the self-help cases, to be "privileged," or justified by a set of circumstances that are difficult to cabin within this yes/no framework. But even after these qualifications are taken into account, chiefly by a pleading system that allows for excuses and justifications for prima facie wrongs, these simple rules prove durable because litmus tests dispose of a very large fraction of actual disputes, so that in practice the recognized exceptions do not drown out the general rule. The opposition between rules and standards is accurately regarded as a spectrum with all sorts of permutations possible between the poles. But in practice sound legal systems cluster closer to hard and fast rules than to the mushy middle gray ground.

To see why this is the case, compare two ways at looking at the law of contract: the first lists all the possible defenses, whether by way of excuse

---

41 *See, e.g.*, John Wade, *On the Nature of Strict Tort Liability for Products*, 44 MISS L.J. 825, 826-37 (1973); *cf.* Richard A. Epstein, *The Risks of Risk/Utility*, 48 OHIO ST. L.J. 469 (1987) (for my critique of this position); *see also* James Henderson, *Judicial Review of Manufacturer's Conscious Design Choices: The Limits of Adjudication*, 73 COLUM. L. REV. 1531 (1973) (for the modern polycentric view). The case law has tended to follow the Wade position. *See, e.g.*, Barker v. Lull Eng'g Co., 573 P.2d 443 (Cal. 1978); Potter v. Chicago Pneumatic Tool Co., 694 A. 2d 1319 (Conn. 1997); *cf.* Linegar v. Armour of America, 909 F.2d 1150 (8th Cir. 1990) (as a notable exception); *see also* RESTATEMENT (THIRD) OF TORTS, § 3 (1998) (seeking to weave between the two extremes).

42 *See* 47 U.S.C. § 271 (1996).

43 Nor is it conceivable in cyberspace. *See* Dan Burk, *Legal & Technical Standards in Digital Rights Management*, 1 J.L. ECON. & POL'Y (forthcoming 2005) (for the sensible observation that in binomial computer world of 1's and 0's rules, even rules with exceptions, work a lot better than standards).

or justification, against the enforcement of promises: infancy, insanity, breach of condition, mistake, frustration, against public policy, and so on.[44] Assume that all of these have at least some substantive validity, and then ask this next question: what fraction of supermarket transactions are invalidated by these rules? Answer: very few, because the system could not work if, say, one percent of all transactions resulted in disputes, even disputes that were resolved short of litigation. The salvation of the system is that higher levels of reliability are obtainable, often by investing in local infrastructure, e.g., the foul pole or receipt, that eliminates the most common sources of controversy. The hugely difficult questions (what is the role of proportionality in limiting the right to use force in self-defense) often remain unresolved for *centuries* precisely because of the happy circumstance that the difficulty of their resolution is belied by the infrequency of their occurrence. The simplest iteration of the overall legal rule is sufficient to resolve the lion's share of the conflicts, which is why they receive the description of the rule of thumb—a measure that is readily available in all face-to-face disputes.

The clear morale of this brief narrative is that a state-of-nature regime of self-help can survive, if at all, only in a world in which the substantive commands are rule-like in form and content. The key element is that the rules that are enforced under a system of self-help have to resonate with the strong intuitive processes that are used to generate moral judgments. The complex standards of the modern administrative state are the wrong place to start for this kind of inquiry. The powerful movement here is toward simple rules for a complex world, not to coin a phrase.[45] One sign of this is the constant reliance on fixed tariffs for certain classes of injuries.[46] These

---

[44] *See* H.L.A. Hart, *The Ascription of Responsibility and Rights*, *in* XLIX *Proceedings of the Aristotelian Society (New Series)* (1949) 171–94, *reprinted in* Logic and Language (First Series) (Antony Flew, ed., 1965), 151–74 (for just this approach); *cf.* P.T. Geach, *Ascriptivism*, 69 PHIL. REV. 221, 221–25 (1960); George Pitcher, *Hart on Action and Responsibility*, 69 PHIL. REV. 226, 226–35 (1960) (for criticisms of the position that Hart found persuasive); *See also* Richard A. Epstein, *Pleadings and Presumptions*, 40 U. CHI. L. REV. 556 (1973) (for my elaboration and criticism of this position); Richard A. Epstein, *The Not So Minimum Content of Natural Law*, OX. J. LEGAL STUD. (forthcoming 2005). Hart was not wrong in seeing that the principle of defeasibility applied to legal analysis. But he was mistaken to think that it went to the issue of meaning, when, in fact, it goes to the connection between description and responsibility. Definitions need not be defeasible. But the gap between the nonperformance of a contract and its breach lies in the fact that the former assertion means that all avenues for excuse and justification have been exhausted, while the latter statement holds that some defense might be interposed, which itself is subject to further exceptions. A similar relationship exists between such terms as "taking" and "stealing" or "killing" and "murder."

[45] *See* RICHARD A. EPSTEIN, SIMPLE RULES FOR A COMPLEX WORLD (1995).

[46] These fixed tariffs are common in most early legal systems even after the rise of the state. *See, e.g., Dooms of Ine*, *in* Sources of English Constitutional History: A Selection of Documents from A.D. 600 to the Present 6-12 (Carl Stephenson & Frederick George Marchan, eds., 1937) (setting out particular fines for particular offenses). *See also Dooms of Alfred*, *in Id.* at 11 § 35 ("One who binds an innocent *coerl* shall pay [him] 10*s.* compensation. One who flogs him shall pay [him] 20*s.* One who puts

tariffs, of course, ignore the variation in individuals, but they have the greater virtue of collapsing the time needed for decision, so that the thread between the incident and its resolution remains both apparent and strong. No system of self-help could survive when the party who loses a particular dispute routinely refuses to accept its moral legitimacy. So with that element, it is useful to go over the basic rules that form the core of the self-help tradition. The next section will explain the extent to which they survive in modern contexts.

D. *Legal Rules for Primitive Self-Help Systems*

1. Autonomy

There is no question that some belief in individual autonomy—which in turn presupposes a continuity of personality[47]—is one of the central principles of the legal system. A rule that gives each person self-ownership is one that establishes clear boundaries that just about everyone can understand. It is not that every person is entitled to do what he wants with his body. That is just an invitation to anarchy. As the late J.W. Harris always stressed, "[i]t is criminal to commit assault or homicide with a weapon, but it is completely irrelevant whether the accused owned the weapon or not."[48] Rather, it is that each person has the exclusive possession of his own body and is the sole person who can decide which of the myriad of permissible actions will be undertaken. The rule is easy to put into place because of the stress it places on the physical invasion of the space of another. Because of the sharp boundary conditions, it is, in general, easy to determine what actions count as a violation of that rule. "Thou shalt not kill" is not the ultimate refinement of a mature legal system, but it is a good place to start. Today, we have powerful criminal and civil sanctions against these forms of behavior, but this rule is the place to begin even in a regime that depends strictly and solely on self-help for enforcement. One correlative of this particular rule is that all individuals are entitled to use force in self-defense. Indeed, how could they do otherwise than honor the overpowering biological instincts for self-preservation so central to the theories of Locke and Hobbes? The mere fact that the community at large looks with disfavor on

---

him under duress shall pay [him] 30*s*.") Note the *coerl*, in contrast to the *earl*, is an ordinary freeman, *Id.* at 3, n.7. The term duress here suggests an awareness of key elements that undermine obligations, but our editors indicate that their translation generalizes from concrete examples that easily fall within the class. In this case, the party charted "locks him up or fastens him in stocks." *Id.*, at 11, n.4.

47 *See generally* JOHN LOCKE, AN ESSAY CONCERNING HUMAN UNDERSTANDING, 204-10, § 10-22 (Roger Woolhouse, ed., Penguin Books 1997) (1690).

48 J.W. Harris, "Who Owns My Body" 16 Oxford J. Legal Stud. 55, 60 (1996). For a more exhaustive statement of his view, see, J.W. Harris, Property and Justice (1996).

acts of aggression has the salutary effect of reducing the frequency of their occurrence. The self-help remedy is, therefore, critically important for all the cases that don't happen, even if they cannot easily resolve all the cases that do happen.

To be sure, this rule is necessarily subject to qualifications, as noted with the reference to privilege. There is always the question of whether retreat is preferable to defense, or whether the use of force continued even after the risk of death or bodily injury had passed. There are enormous problems that arise when individuals seek to use force before they are attacked or use it to help defenseless third parties. But none of these admitted complexities should deflect us from the central point: in a world in which all persons internalize the Hobbesian imperatives, no social practices against aggression and in favor of self-defense could emerge. But in a world with some degree of emotional empathy and connection, the overall system will do better than with some randomly chosen rules. There is some brief level of respite even in a state of nature.

2. Acquisition of Property

A similar analysis helps apply self-help to the rules of property. The standard rule in all primitive societies is that land, animals and particular objects all become the property of the first person to possess them. That person is then in a position where it is legitimate for him (and his allies) to use force to defend his possessions against the attack of others. One striking characteristic of the rule is that it does not matter how large or small the time gap between the first possessor and his subsequent rival. The race is strictly ordinal, the size of the gap matters no more here than it does in deciding who wins an Olympic gold medal—the British men's 400 meter team in the Athens 2004 Olympics did not split their prize with the Americans, whom they beat by 0.01 second. This clarity is of critical importance because it means that single variable is all that anyone needs to know to determine which of two rival claimants is the owner of a particular thing.

Yet more is at stake. The operative sense of the rule is not confined to an ex post resolution of close cases in which two or more persons may be in hot pursuit of the same object. The key point to understand here is that property rights are supposed to be good against the entire world. 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. Like the principle of individual autonomy, this rule forestalls disputes precisely because other individuals tend to strongly accept the overall legitimacy of the system and are, therefore, more reluctant to enter any territory where someone else has already staked a claim.

This overall system, moreover, may well be strengthened by an inbred psychological disposition to be more aggressive in defending turf than in

taking it over. There is some evidence in animal behavior to the effect that animals will by and large respect the territories of others when staking out their own claims. Thus, the signaling methods used by people have a long evolutionary history, which is sufficient to allow the emergence of some modest system of property rights. Indeed the much vaunted, if elusive, endowment effect may well be at its maximum here.[49] Here is one example that illustrates the point: cones of light are sources of energy for the speckled wood butterfly.[50] The cones are of short duration, and only one butterfly can occupy a typical cone at one time. Yet the following behavioral patterns are observed. Let butterfly A take over the cone, and butterfly B, the interloper, will fly away if challenged. But reverse the positions of the two butterflies and B will prevail as the new incumbent. When each thinks itself the incumbent, they will engage in a prolonged struggle for the cone, the expected value of which is probably negative for the pair. The point here is that the first possession rule works as a powerful sorting device that in most cases avoids conflict.

The same set of emotions seems to govern human behavior. If a man has a rush of adrenalin when he takes possession of a particular thing, then he is more likely to be willing to defend it relative to some outsider who attaches a lower value to the same object. Or perhaps the explanation lies in the fact those who think that their claims are legitimate are willing to struggle harder than those who know they are interlopers. Whatever the precise explanation, it appears that the full range of possession rules does work passably well to sort out property claims even in the absence of any form of central authority. And there is little doubt that this rule which applies to contests between individuals, can apply to contests between nations, which helps explain why, more often than not, borders between rivals turn out to be stable in many cases. It is only when the imbalance of power becomes acute that the risk of invasion becomes large, and then some triggering event is often needed to justify the invasion in the eyes of the world, even if it is fabricated for the occasion.

The articulation of this norm of prior possession necessarily gave rise to enormous debates over the content of the proposition "A possesses X." The simple matter here is whether one keeps possession of his item when he lets it out of his grasp, to which the functional answer has to be yes, lest the acquisition of new goods is rendered impossible by the need to keep a constant hold on other possessions.[51] The cynic might say, why the worry

---

[49] EPSTEIN, *supra* note 44, 219-29 (for a discussion of why the effect makes more sense in acquisition cases than in transfer cases).

[50] *See* N. B. Davies, *Game Theory and Territorial Behavior in Speckled Wood Butterflies*, 27 ANIMAL BEHAV. 961–62 (1979); *see also* John Maynard Smith, *The Evolution of Behavior*, 239 SCI. AM. 176, 191–92 n.3 (Sept. 1978).

[51] For a simple discussion of the evolution of the idea of possession, see BARRY NICHOLAS, AN INTRODUCTION TO ROMAN LAW 112-14 (1962) ("For obvious reasons of convenience the requirements

about the duration of possession, given that other individuals will take advantage of their opportunity to take anything that is left unprotected. As Hobbes famously noted, people lock their doors precisely because they fear the attacks of others, from which he famously concludes "Does he not there as much accuse mankind by his actions, as I do by my words."[52] But again all this misses the point about differential levels of aggression in various individuals. The Hobbesian quote, in people "accuse" mankind, does not necessarily mean that people accuse each person of bad motive. The clear implication of Hobbes's statement is that he thinks that the *first* person who walks by the unlocked door will remove the contents from the home. But the far more common reaction would be for the random stranger to lock the door for the owner in his absence. It is for just this reason that it is always better to lose goods than to have them stolen, for chances are that the finder will return them to the owner or to that venerable non-Hobbesian institution, the lost and found.[53] The correct analysis, therefore, asks how many individuals it will take before a single one decides to enter the house and steal. Thus, it is perfectly rational to lock your doors even if you think that only one person in a thousand would break the moral code against theft. The decision to lock the doors is driven by the behavior of the *worst* person or persons in the crowd, not that of the median. Indeed, in many close-knit communities that risk seems to be worth running, for doors are left open. The common man's understanding of self-interest is far better (if less profound) than Hobbes's. People are in varying degrees and settings self-interested, but only to the extent that they can advance by playing within the rules of the game. They are only "pragmatic" within the rules; they are not "pragmatic" about the rules.

3. Contract

The concerns with self-help also permeate the law of contract, where even in mature legal systems, legal enforcement is much the exception.

---

of the law are not so strict for the retention of possession as they are for its acquisition. I do not lose possession of my house and its content merely by going away for a short time, nor do I lose possession of a book which I have put in a cupboard and forgotten."). *See also generally* H.F. JOLOWICZ & BARRY NICHOLAS, A HISTORICAL INTRODUCTION TO THE STUDY OF ROMAN LAW (1972). The point has real relevance to the evolution of modern property theory, on which see JEREMY BENTHAM, THEORY OF LEGISLATION 111-13 (4th ed. 1882).

52 THOMAS HOBBES, LEVIATHAN ch. 13 (1651). I critique this passage in RICHARD A. EPSTEIN, FORBIDDEN GROUNDS: THE CASE AGAINST EMPLOYMENT DISCRIMINATION LAWS 17-19 (1992).

53 One personal illustration. About ten years ago, I took my then 9-year old son Elliot and his friends to a baseball game at the then-Comisky Park. One of the boys had to use the stalls in the men's room, where he left his small backpack, which we discovered only ten minutes later. So we went back to the stall, where it was not found, and then on a hunch went to the lost and found, which was located about 500 feet away. Sure enough, some total stranger had turned it in anonymously. Crisis averted.

The key feature for making the system work is a clear sense as to when the obligation begins and when it does not. The earlier emphasis on formality to conclude a deal performs just that function, as with the Roman contract of stipulatio, which was formed by the use of the same words in a question and answer format.[54] The English seal serves the same function.[55] Formality of whatever type demarcates negotiation from agreement, and reminds people of the seriousness of the transaction. We still use similar devices to this very day: the handshake and the signature have just this function. The voluntary exchange cannot survive in a self-help regime in the face of persistent, deep disagreements on whether the promises were made in the first instance.

The use of formalities does not, of course, solve all problems. There is still the question of performance: will the other party make good on the promise? (Or, in truth, will I?) But it hardly follows that *all* forms of cooperation will cease because of the risk of defection, as the Hobbesian model predicts. People get to choose their trading partners, and therefore can gravitate away from the dubious partners. They do not have to run the risk that one in a thousand will enter their homes. They need only be confident about the trading partners who are selected in part for their probity.

To be sure, there are risks even in this context. Against these perils, the simplest form of protection is a simultaneous exchange in which each side gets to inspect the goods or services provided by the other before going through with the deal. There is little question that the ideal theory of contract law would protect the expectation interest on each side, i.e., the gain that one hopes to get through the ordinary completion of the trade. But it is equally likely that this remedy could never be enforced in a regime limited to self-help. Rather, the simpler remedy for the buyer is *rejection* of the nonconforming goods, while the dominant remedy for the seller is a refusal to make further deliveries until past bills were paid. (The political analogy is the exit right, which is more costly to exercise because the citizen has to give up lots of local benefits to escape the sovereign.) These self-help tactics do not provide optimal incentives to perform, but they do share this desirable characteristic. They leave the party in breach (who has expended some effort and forgone other opportunities) worse off than if the exchange has gone through. We should, therefore, see at least some trade emerge without legal enforcement, especially if there are interests that link the two sides together, e.g., common relatives who can broker the deal.

The situation gets more difficult when the exchange takes place sequentially, that is, when one side performs before the other. But once again

---

[54] For a brief discussion, see BARRY NICHOLAS, AN INTRODUCTION TO ROMAN LAW 193-94 (1962).

[55] *See*, for the English requirement, SIR JOHN BAKER, THE OXFORD HISTORY OF THE LAWS OF ENGLAND, VOLUME VI, 1483–1558 814, 822 (noting that in England, many types of contracts had to have a seal, which, when present, made for limited obstacles to liability).

these trading systems do not suffer a total meltdown. The potential for long-term gain may be sufficient to induce individuals from taking what is left in the first round. Hence, one strategy is to reduce the quantities that are traded so that they are always smaller than the anticipated gain from the maintenance of the relationship. That argument works, moreover, without any reference to empathy or sentiment. But it hardly falsifies the view that these elements are irrelevant to the system of trade, for nothing precludes the possibility that these two motivations are cumulative. Quite simply, the amount that one puts at risk can be somewhat larger because there is some confidence that others will not renege on transactions because they can make, on net, some small gain amount. The impulse to cooperate thus expands the size of individual trades, and reduces the number of trades needed to reach some fixed target.

There is yet another mechanism that strengthens the hand of self-help regimes among traders: the choice of who becomes a trader. One defect of traditional rational choice theory is that it assumes that there is no variation among individuals on the question of egoism. Everyone operates in more or less the same fashion. But levels of self-interest are not immune from the general rule that all large populations exhibit some variance over any natural trait. Since trust is at a premium in these relationships, we should expect some comparative advantage to people with two sorts of traits. First, the willingness to abide by the moral norms of exchange even in the absence of an enforcement mechanism. Second, an ability to detect cheaters who would otherwise upset the balance of this operation. Thus, the nature of the key personalities will heavily influence the success of the enterprise. Since the narrow egoist is much more likely to bolt than the trader with some moral sense, we should expect to see more of the latter in this regime than the former. It is exactly on this point that the differences in world view matter so much in the prediction of human behavior. Those who believe that the moral sense sometimes guides decision can easily conceive of situations where people honor commitments which they could breach with impunity, even if the temptation of easy gain is too great for others, who opt for the short-term gains from breach. It is just this last, narrow attitude that informed the Holmesian "pragmatism" that treats a contract as a simple option to perform or to pay damages.[56] This "pragmatism," of course, provokes strong reactions in people with ordinary moral sensibilities, for whom an option not to perform is one thing and an obligation to perform is quite the other. It is for just this reason that ordinary people react with stunned disbelief when told of the economic theory of "efficient breach," which is an oxymoron in traditional discourse: efficiency is a trait to be prized, but breaches are by definition wrong.[57] To collapse them into a sin-

---

[56] *See* OLIVER WENDELL HOLMES, THE COMMON LAW 301 (1881).

[57] *See, e.g.*, Daniel Friedmann, *The Efficient Breach Fallacy*, 18 J. LEGAL STUD. 1 (1989). Another way to put the objection is that the expectation measure of damage gives all the benefits that flow

gle phrase misses the essential distinction that some people will bargain as hard as they can in order to get the advantage under a contract, but will scrupulously honor the agreement once it is made. Self-interest is a powerful force, but it is one that for many people operates within the framework of the legal rules. To elide this difference is to weaken the social fabric that helps to reinforce the shaky social norms that make self-help, and social life, possible.

II. SELF-HELP IN CIVIL SOCIETY

A. *Generally*

The situation as it exists in any state of nature is, of course, fragile because it requires each individual to execute the law of nature on his own behalf. For without self-help, "the *law of nature* would, as all other laws that concern men in this world, be in vain, if there were no body that in the state of nature had a *power to execute* that law."[58] The cynic would say that this observation is of no consequence because each and every individual could hide his aggressive schemes behind the "execution" of the natural law. But if the argument made above is correct, the decision for self-enforcement, while far from ideal, will be better than random, and will be commonly marked by a willingness to limit the imposition of sanctions to the frequency and severity of the harm so caused. There is no question that this system leaves a good deal to be desired, which is why Locke (and, for that matter, almost everyone else) sees the need to create some state with the power to appoint neutral and impartial judges to resolve these disputes and to stop the cycle of private vengeance before it starts.[59]

The question then arises what adjustments should be made to the substantive rules developed by individuals in a state of nature for governance

---

from breach to the party that has created the wrong, even if it is perfectly enforced. Worse still, in practical contexts, it is difficult to trace out all the damages that flow from nonperformance, especially for people whose business transactions with third persons are made more costly in consequence of breach. This ripple effect is one reason why the traditional view, *pacta sunt servanda* (promises must be kept) is so important. The performance of one contract reduces the probability of a nasty dispute over whether the nonperformance of the next deal counts as a breach or is excused by the prior breach of this party. The standard economic accounts ignore this dynamic element.

58 JOHN LOCKE, THE SECOND TREATISE ON CIVIL GOVERNMENT 10 (Prometheus Books 1986) (1690) (emphasis added).

59 *See id.* at 13 ("*[C]ivil government* is the proper remedy for the inconveniences of the state of nature, which must certainly be great where men may be judges in their own case, since it is easy to be imagined that he who was so unjust as to do his brother an injury will scarce be so just as to condemn himself for it.") (emphasis added). Locke thought the requirements of justice, "an *established,* settled and known law" as enforced by *"a known and indifferent judge,"* with *"power"* to implement its rules. *Id.* at 70.

in a civil society. It should be recognized at the outset that a regime of stable and impartial judges marks a huge advance in social life.[60] But that observation does not say whether the substantive rules best suited for a self-help regime should be jettisoned for something else. In some sense, the answer to that question has to be yes, given that the state must establish the system of courts and devise their rules of criminal and civil procedure. But that answer is not exactly responsive to the underlying inquiry, which only asks whether the movement from a state of nature to a civil society changes the *substantive* principles of autonomy, property, contract and tort that offer the best chances for success in a state of nature.

Here the answer runs, I think, as follows. As a matter of first principle, the rules that allow for the creation of private zones of liberty and property carry over to civil society *without missing a beat.* These rules favor positive sum interactions from a baseline of well-defined property rights. There is no obvious reason to prefer a set of entitlements that give all (or most) individuals rights of housing, education, health care, and the like, against their fellow citizens. Rather, the advantages of the old rules should be supplemented only by changes that help to regularize the preferred transactions in a self-help world. Self-help in a Lockean framework is what each person "*gives up* to be regulated by laws made by the society, so far forth as the preservation of himself and the rest of society shall require."[61] The regulation in question is done "to unite, for the mutual *preservation* of their lives, liberties and estates, which I call by the general name, *property.*"[62]

This surrender of power was meant to preserve just those rights in the state of nature. The regulation of property did not mean rent control: it meant that systems of deeds and recordation could be introduced to improve the stability of transactions without undermining the basic logic that voluntary exchanges produce mutual gains. Indeed, my own guess is that Locke was thinking of the great English law reform of the seventeenth century, the Statute of Frauds of 1677.[63] But once that point is recognized, why assume that any judicial system will work better with blurry rules and ad hoc standards than it will with the simpler rules that make it possible to monitor and enforce a self-help regime? The starting points, therefore, are remarkably similar.

The question then arises as to what improvements, apart from such formalities as deeds and recordation, could improve matters within civil

---

[60] As Jared Diamond notes in GUNS, GERMS, AND STEEL, every population of over 50,000 people develops a judicial system—whose complexity, I might add, increases at a lower rate than population.

[61] *Id.* at 71.

[62] *Id.* at 70.

[63] An Act for the Prevention of Frauds and Perjuries, 1677, 29 Car. 2 c.3, 8 Stat. at Large 405 (Eng.).

society. On this score, substantial improvement is possible.[64] 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 expenses for a greater return, that is fine. Thus, the public system supplies an extra option, not an obligation.

There is much to be said for that position. For example, suppose one self-help remedy allows an individual to build a wall to make sure that others do not invade his privacy. Why should any court discourage this self-help remedy against snooping because it makes available an action for the invasion of privacy? Similarly, suppose that the standard self-help remedy in contract is to refuse to perform your half of the bargain if the other side has failed to perform its half first: no one has to pay for goods that have not been delivered, for example. It would be grotesque to foreclose that option and to force the innocent party to sue in contract for expectation damages. The innocent party gets the options. For example, after a defendant's anticipatory breach, the plaintiff may disaffirm the contract immediately, a self-help remedy, or wait until performance is due before disaffirming (at least if no reliance costs are incurred in the interim).[65] Or he could sue for damages initially, or wait until performance is due. I have little doubt with most small transactions the cheap self-help remedy dominates. It is only

---

[64] I put aside here one *enormous* caveat, which is the development of the full range of institutions designed to deal with monopoly and common pool problems, which of course could not be addressed and overcome in the state of nature. I have no desire to minimize the scope of these rules, for as a general principle, I think that anytime someone can suggest a redefinition of property rights that produces a strong Pareto improvement over the common law distribution of rights, it ought to be accepted, just as the acceptance of taxation to support the common law rights of liberty and property should be accepted. See, *e.g.*, Richard A. Epstein, *One Step Beyond Nozick's Minimal State: The Role of Forced Exchanges in Political Theory*, 21 SOC. PHIL. & POL'Y 286 (Winter 2005), for one discussion of a theme that lies in my view at the heart of political theory. But for obvious reasons, I will not discuss those points here, as they do not impinge on the analysis of self-help as it applies to traditional rights of person and property.

[65] Hochster v. De La Tour, 118 Eng. Rep. 922 (1853) (allowing the immediate suit or withdrawal from the contract). The leading authority to the contrary is Daniels v. Newton, 114 Mass. 530 (1874) (rejecting the right of the immediate action by allowing the self-help remedy of withdrawing from the contract).

when the stakes get large that the expected payoff is large enough to warrant suit.

It is important here to take note of a general feature of both these situations, and many others like them: the use of self-help remedies (by building walls on one's own property or treating a contract as rescinded) do *not* involve the use of force against another person. So there are no negative spillover effects that caution against using the cheaper but less complete, self-help remedy. Yet in some settings, the apparent self-help remedy may in fact operate as a wrong against the other side. If, for example, a neighbor has a covenant against new construction, building out for privacy is a breach of that right. If the second party chooses not to perform when the first one in fact has done its part, the purported self-help is in reality a breach of contract. At this point, the so-called innocent party might be given the option to rip down the wall or to snatch back goods after delivery. But now the use of force as a self-help remedy carries with it two important risks that have to be endured in a state of nature, but not necessarily outside of it. The first is that the use of force in question is not justified, so that what passes for self-help is in fact an aggravation of the original wrong. The second is that the action is in fact justified but brings in its wake several unfortunate consequences. Either it will provoke a violent reaction by the aggrieved party or it will expose innocent third parties to risk of bodily harm or property damage.

It is for these reasons that the standard account of self-help routinely imposes various "reasonableness" limitations on the doctrine, forcing individuals to go to court when these are pronounced.[66] Indeed, the overall pattern is both simple and effective. Individuals are generally allowed to exercise rights of self-help in those cases in which there is no risk of immediate physical confrontation. However, the price that they pay for that option is a possible countersuit by the other side, which may well carry with it the prospect of more than simple damages. Nevertheless, in some cases the fear of harmful interaction is so great that self-help is banned altogether.

A couple of historical cases help to illustrate the basic pattern. One class of cases involves the medieval remedies to recover real property.[67] After a dispossession, the disseised party was allowed a period of four days in which to use the self-help remedy. The decision to confine the remedy to that time period reflected that four days was long enough to allow the owner to rally his friends about him, but not so long as to blur the underlying merits of the dispute. But if that period failed, then the next remedy

---

66 See the various rules, RESTATEMENT (SECOND) OF TORTS, §§ 63-76 (1969).

67 For the classic exposition of these rules, see 2 SIR FREDERICK POLLOCK & FREDERIC WILLIAM MAITLAND, THE HISTORY OF ENGLISH LAW BEFORE THE TIME OF EDWARD I 49-62 (The Lawbook Exchange, Ltd. 1996) (2d ed. 1898). For a shorter account that does not discuss the self-help portion of the matter, see F.W. MAITLAND, THE FORMS OF ACTION AT COMMON LAW 20-40 (A.H. Chaytor & W.J. Whittaker eds., Cambridge University Press 1936) (1909).

was novel disseisin, whereby the displaced tenant sued to recover the premises in a summary procedure that excluded, at least at the outset, the defendant from raising any affirmative defenses to the case. But the defendant who lost on the writ of novel disseisin could in turn bring the slower and more cumbersome writ of right. At that point all the issues of title could be negotiated. Hence, the plaintiff in the writ of right could allege that he had indeed disseised the defendant, but only because the tenant had previously disseised him. The basic pattern is both simple and enduring. The quick procedures are tolerated so long as they are backstopped by more complex rules. In the case of the English real actions, novel disseisin became so cluttered procedurally that it eventually fell by the wayside.

There are echoes of this pattern in the modern law of landlord and tenant. The landlord was traditionally allowed to evict his tenant on expiration of a lease or for a material violation of its terms.[68] This self-help remedy, which allowed the landlord to repossess the premises, at the margin increased the willingness of landlords to rent in the first instance, or lowered the rent they demanded. But the privilege of self-help could not be exercised in the face of determined resistance; if that happened, the assistance of a sheriff was required.[69] But when self-help was used, then the tenant could sue afterwards to contest the legality of the eviction. The two-part system reduces the probability of an improper eviction by landlords who, since their identities are known, can be sued for substantial damages. The hard empirical question is whether to risk eviction, and disorder, by self-help at all. Here it depends on the efficacy of alternative procedures. Sometimes the law provides summary procedures that allow for a quick eviction. These typically take the form that limit defenses to a narrow class of issues, such as whether the tenant has not paid the rent. If this procedure is executed in a quick and effective manner, then why not require it? But if it leaves a tenant in possession when there is a risk of wrecking the premises, then it is a bad trade. As with all of these cases, the trade-offs turn on empirical hunches. The modern tendency is to cite the reliable procedures for summary eviction as a reason to impose a per se ban on self-help.[70] My own attitude is in general to require some clear showing of generalized abuse before cutting out the self-help remedy. To knock it out because

---

68 *See* Vanderbilt Special Project, *supra* note 2, 860-65. *See, also*, Hemmings v. Stoke Poges Golf Club, Ltd., 1 K.B. 720 (Eng. C.A. 1919), (denying the evicted tenant a remedy even when the landlord's conduct violated the applicable criminal law, on the ground that no private wrong had been committed if the transaction was properly executed).

69 *See* Allen v. Hannaford, 244 P. 700 (Wash. 1926) (holding that a landlord could not use force to threaten the plaintiff who had removed her furniture from defendant's apartment, even though the defendant had a lien on the property for the payment of back rent).

70 *See, e.g.*, Berg v. Wiley, 264 N.W.2d 145 (Minn. 1978) (modifying earlier decisions that had allowed peaceable dispossessions, claiming that no such dispossession could be peaceable because they always held out the risk of violence).

abuse might occur seems to be an overreaction. There should be at least some pattern of cases that indicates the risk of breakdown to social order.

Similar rules apply to the recaption of chattels, where the general rule allows a defendant to make hot pursuit of someone who has run off with his goods.[71] The usual requirement is that the goods be taken by force without any claim of right. This formulation precluded the invocation of the privilege in *Kirby v. Foster*,[72] where the defendant employer entrusted the plaintiff, his bookkeeper, with money for the payment of the help. On the advice of counsel no less, the plaintiff deducted his own salary plus an extra $50 he claimed the defendant owed him and returned the rest. The defendant then used force to wrest the money from the plaintiff, causing injuries. The defendant's privilege of recapture was rightly denied, because the defendant had injected a new element of force into the transaction.[73] Here the sum taken was limited to a claimed debt, so there was no unbridled use of force. The defendant knew where the plaintiff was and how to find him. It is the perfect case to require the defendant to refrain from self-help and to use legal processes that should, if the claim were sound, give the defendant-employer something above and beyond the value of the money unlawfully retained by the plaintiff-employee.

The topic of recaption of chattels just covers a small corner of the entire area of self-defense and defense of property, where the stakes are often higher on both sides. To ask an innocent party (if we know who he is) to refrain from the use of force when threatened with serious bodily harm or the substantial loss of property is to demand too much, and to increase the chances of such aggression. In most cases, moreover, it will be clear who started the attack: the ruffians with criminal records, not the couple running home on a dark night. But the usual case is not the invariable one. Although the scope of the privilege expands to take into account the increased nature of the harm, it is not carte blanche. The man who steals the wallet with $10 and runs away may be pursued, but not shot. The risk of excessive force and the danger to third persons is just too great.

An intermediate case involves situations where a defendant seeks to abate a nuisance caused by the plaintiff.[74] Here the noxious fumes and the like surely justify for legal relief; but the interim discomfiture and dangers to health or livestock may be hard to quantify. So self-help is allowed even if the remedy of abatement necessarily involves a trespass on the defendant's land. But again the usual conditions about resistance from landowners and harms to third persons hold in this context as in all others. There

---

71 *See* RESTATEMENT (SECOND) OF TORTS, § 101 (1969); Vanderbilt Special Project, *supra* note 2, at 863.

72 22 A. 1111 (R.I. 1891).

73 *See id.* at 1112.

74 Vanderbilt Special Project, *supra* note 2, at 853 n.13 (noting that the rules are more or less the same for self-defense and recaption of chattels), and, more extensively at 868-70.

had better be, as it were, cyanide in the air to allow the immediate use of force without calling on public officials for assistance.

B. *In Cyberspace*

The issues regarding the use of self-help in traditional contexts have proved stable over recent years. It is difficult to find a new appellate decision that raises novel issues on this point—at least until the advent of cyberspace. The fundamental premise of this Conference is that cyberspace raises the most modern challenges to the law of self-help. To be sure, we do not have to deal with cases of physical violence in the duels that take place between the individuals who mastermind the vast number of computers and sites that remain connected in cyberspace. But there is little doubt that the issues of hacking into computers (and wrecking their content), spamming computers, so that they become overloaded with unwanted materials, and using unwitting computers, typically called zombies, to spread spam across the network in ways that make it difficult if not impossible to trace back to its original sources, all raise self-help concerns.

In this short discussion, I shall not attempt to resolve the issues in question, but only wish to point out the eerie similarity to the problems that self-help raised in earlier times. In many cases, there is no central authority that can deal with the various incursions that routinely take place in cyberspace. The network is surely global, which means the worst offenders to the system can easily reside outside the jurisdiction in which they wreak their harm. The inability to get powerful state remedies thus puts the emphasis back on the self-help remedies. In dealing with self-help, it is important not to lose sight of the fact that most users of the Internet happily avoid the use of any of these dubious techniques. But the problem is so intractable because it takes only a small group of *anonymous* individuals to disrupt the operation of the entire system. At this point, the level of informal sanctions that prove so critical in a state of nature are much weaker in cyberspace. What then remains to be done? Here there is no one who thinks that it is improper for individuals to take defensive measures to keep unwanted intruders from entering a web site. Gated communities that are found in real space have their precise parallels in cyberspace, as individuals seek to economize on the costs of cyber security by banning together and hiring experts to supply protection for them.

The inability for these measures to work raises the stakes. My colleague, Douglas Lichtman, arrays the full range of possibilities for self-help in cyberspace, in the hopes that further work will pick the best alternatives. Henry Smith then addresses the question of whether property owners should have a right to exclude or whether some state system of governance should decide which uses an owner may exclude, and which not. David

McGowen addresses this question in the context of the important case of *Intel Corp v. Hamidi*,[75] in which the California Supreme Court denied injunctive relief for the familiar tort of trespass to chattels in the absence of any showing of disruption of computer operations or physical damage to the website. I shall add my own further views on that case as well.

The relevant issues are not so narrowly confined, for other techniques to deal with the dangers to the internet have also been bandied about. One specific possibility is to develop some general architecture that (like streetlights) exposes wrongdoers to social sanctions. Neal Katyal has proposed this sort of scheme, but its effectiveness has been doubted in this issue by Orin Kerr. Yet another more aggressive approach discussed in Bruce Smith's paper, involves the iSIMS program which allows a computer to reach out and attack other computers that are determined to have attacked it. Note the issues that this aggressive approach raises. What should be done if the program picks up the wrong target and wrecks the computer of an innocent party? What should be done if the attacked target is a zombie computer that has unwittingly transferred the offending material across cyberspace? Are there any limits of proportionality that are associated with these attacks? Should the self-help remedy be denied on the grounds that some form of civil liability could be imposed? If so, should that liability be restricted only to the willful wrongdoer or should it extend to responsible intermediaries, such as Internet service providers who may have the ability to track down some of the deliberate wrongdoers, but who may also be overwhelmed by the literally thousands of requests (some no doubt bogus) for assistance that will come their way if they can be held liable? Here these questions cannot be fully answered, I suspect, without dealing with the tort/contract interface that has proved so important in product liability cases. Could an ISP, for example, contract out of any liability with its subscribers, just the way that water companies can contract out of liability for the damages that result when their systems fail?[76] The permutations are well-nigh infinite. The level of social consensus is low. Clearly, we all have our work cut out for us.

---

[75] 71 P.3d 296 (Cal. 2003).

[76] For an example of the basic problem, see Weinberg v. Dinger, 524 A.2d 366 (N.J. 1987), which evaluated one such contract, which limited the obligation "to use reasonably diligent efforts" to correct the situation. Query whether this will suffice.

COMMUNITY SELF-HELP

Neal Katyal[*]

This paper advocates controlling crime through a greater emphasis on precautions taken not by individuals, but by communities. The dominant battles in the literature today posit two central competing models of crime control. In one, the standard policing model, the government is responsible for the variety of acts that are necessary to deter and prosecute criminal acts. In the other, private self-help, public law enforcement is largely supplanted by providing incentives to individuals to self-protect against crime. There are any number of nuances and complications in each of these competing stories, but the literature buys into this binary matrix.

The community-based solution proposed here incorporates aspects of each model. By "community" self-help I mean to distinguish self-help from the spontaneous action of individuals as a response to crime. Instead, I employ the term to mean acts of group self-help that are coordinated with the government instead of being entirely exogenous to them. Community self-help therefore balances goals of both public and private enforcement. For instance, a chief advantage of a public enforcement solution, as we shall see, is that it avoids the atomization prompted by individualized self-help. But such solutions are often inefficient, cost far too much, and do not adequately prioritize resources. If the law encouraged community-based self-help, however, it could permit resources to be targeted toward those areas that need it the most, and also foster greater interaction instead of isolation.

A community-based model of law enforcement has been taking off in the past few years in America, as "community policing," "community prosecution," and "community courts," become more common. But that trend has not spilled over into either theoretical analysis or practical application of how the community perspective might inform analysis of self-help. This paper attempts to fill that gap. It argues that the concept of "self-help" should be conceptualized in broader terms than subsidizing or encouraging self-help by individual actors. Instead, efforts should be made to encourage community-based solutions in those areas where self-help yields efficient results.

In essence, a community self-help model starts by admitting that neither the public nor the private sector can solve crime, and then asks what mechanisms will best structure dialogue between the two spheres so as to generate a dynamic response. Lone private actors who try to take matters into their own hands will not be trusted, and their success in reducing crime

* John Carroll Research Professor, Georgetown University Law Center.

(if they have it) will often come at the expense of bolstering the fear of crime instead of minimizing it. The same is true of the government. Law enforcement crackdowns on crime can fray a community, producing counterproductive results. But methods that try to create collaboration between private and public enforcement have the potential to promote trust and permit greater social networks to flower. And that collaboration may have spillover effects more generally, increasing the level of dialogue on a host of other issues that affect the community and bolstering political participation.

One lesson from academic analysis of crime control is that community self-help will be most promising when it focuses not on *prosecution* or *retribution*, but rather on *prevention*. Unfortunately, much of our image of self-help is focused on the former, particularly the vigilante, and does not fully consider the virtues of prevention as a strategy. But community policing is now starting to move into the prevention mode, and a variety of reforms in this direction hold promise. Because government institutions guide community-self help initiatives, these strategies are more likely to channel self-help into productive areas. With individual self-help, by contrast, the risk of excessive vigilantism is omnipresent.

One payoff from thinking about crime prevention in this way is that it will help inform the structure of what private precautions in cyberspace should look like. It has become a truism that cybersecurity requires partnering with the private sector.[1] In these kinds of conferences, one hears this phrase so often that it appears that everyone is reading from the same script. But the tough question is of course not whether private precautions are necessary, but what they should look like and how should they be encouraged. There has been a paucity of thinking about that, and this paper attempts to start that dialogue by identifying a set of private solutions that have worked in realspace. By isolating a type of self-help not carried out by lone-actors, a fruitful area for cyberdefense emerges.

I. THE SELFISHNESS OF SELF-HELP

A. *In Realspace*

Begin by isolating the harm of crime. The standard view is that criminal acts are understood as harms to individual victims, but that story is in-

[1] "[F]ederal regulation will not become a primary means of securing cyberspace" and "the market itself is expected to provide the major impetus to improve cybersecurity." *The National Strategy to Secure Cyberspace*, at 15 (2003), *available at* http://www.whitehouse.gov/pcipb; *see also id.* at xiii ("The federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts.").

complete. In particular, crimes fragment communities by increasing fear and reducing connections between residents. In realspace, it has been well understood that in areas where crime is rampant, people do not talk to each other and social organization suffers. "People stay behind the locked door of their homes rather than risk walking in the streets at night. Poor people spend money on taxis because they are afraid to walk or use public transportation. Sociable people are afraid to talk to those they don't know."[2]

The actions described in the above paragraph are all examples of self-help. All have the potential to be purely rational reactions by potential victims to the threat of crime. Proponents of individualized self-help, however, respond by claiming that the key is to encourage incentives *ex ante* for private precaution. By reducing crime rates, the strategy goes, alienation is reduced. While geographic mobility and other phenomena diminish the effectiveness of such strategies,[3] it is possible that some forms of self-help will lower crime without prompting greater isolation. And it is of course realistic to think that such self-help will be far cheaper than public law enforcement.

Here is an example I used here a few months ago to illustrate the point: a woman parks her car on a city street, eats at a restaurant, and emerges to find that her car has been stolen. The police, due to budget constraints, tell the woman that they do not investigate such crimes, and even decide to announce a policy to that effect. In addition to conserving scarce enforcement resources for more serious crimes, the police reason, not without some justification, that the announcement of a policy that they will not investigate auto theft will actually *decrease* the amount of automobile theft. If the police do not protect against the crime, they reason, the numbers of people who own automobiles and drive will be fewer. And those that do drive will take special precautions to guard against theft – from locking their doors to buying fancy electronic anti-theft systems.

---

[2] PRESIDENT'S COMM'N ON LAW ENFORCEMENT & ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 132-44 (1967). Similarly, Bursik and Grasmick note that:

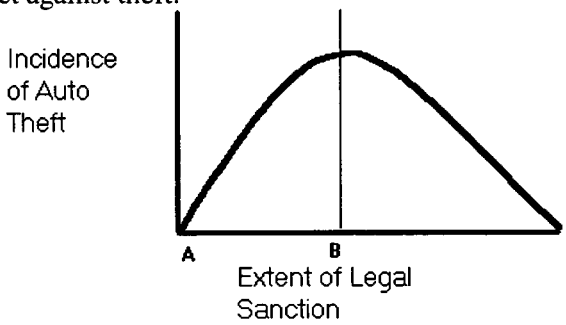
> If such withdrawal from local networks becomes widespread, the sense of mutual responsibility among the residents is undermined, and those who are able to do so may attempt to physically abandon the neighborhood at the earliest possibility. As a result, the capacity for local control may further deteriorate, thereby accelerating the processes that originally gave rise to crime.

ROBERT J. BURSIK, JR. & HAROLD G. GRASMICK, NEIGHBORHOODS AND CRIME 4-5 (1993) (citation omitted); *see also* WESLEY G. SKOGAN, DISORDER AND DECLINE 49 (1990) ("[C]ertain disorders are self-propagating—once they appear, they generate more disorder unless they are quickly and energetically stamped out.").

[3] SKOGAN, *supra* note 2, at 13

> Such withdrawal tends to reduce the supervision of youths, undermines any general sense of mutual responsibility among area residents, and weakens informal social control. Withdrawal also undermines participation in neighborhood affairs, presaging a general decline in the community's organizational and political capacity. . . . Fewer people will want to shop or live in areas stigmatized by visible signs of disorder; these problems feed upon themselves, and neighborhoods spiral deeper into decline.

As this example underscores, legal sanctions against crime are not driven exclusively by the harm of the criminal act. Indeed, the incidence of auto theft may *increase* with legal protection because the absence of law enforcement means that very few will own cars and those that do will self-protect against theft:



The space between points A and B represent the hidden problem of criminal sanctions – the space in which increasing the legal sanction on auto theft has the somewhat perverse effect of increasing it. Some might be tempted to reason that, as a result, the government should stay out of the business of policing auto theft altogether. To get the incidence of auto theft back down, it would take a massive amount of criminal sanction. Instead, the argument goes, let individuals be responsible for their property. This argument can be made with most types of crime: Do you fear credit card theft on the Internet? If so, then abandon enforcement of laws against theft and fraud on the Net. If government did not enforce these laws, then no one would use their credit cards, and the theft would disappear.

But governments of course do not think that way. Indeed, they consistently risk the creation of the space between point A and B. The reason why governments act in this seemingly counterintuitive way has everything to do with the costs and distributional effects of private precaution. If the method to reduce auto theft is minimizing the numbers of cars on the road, that strategy will have all sorts of costs exogenous to crime rates – costs incurred because the automobile has become a fixture of life for many. If, by contrast, the way auto theft is reduced not by less driving but rather by expenditures for better security systems (car alarms, The Club, and the like), then it will raise severe distributional concerns. (Notably, these concerns do not disappear even if private ordering is more efficient.) If only the more wealthy can afford the private protection strategies, then they will be able to drive while the poor will not.

The criminal law exists, in part, as a subsidy to poorer elements in a community. If everyone had to fend for themselves to prevent crime, the richer in society would be able to externalize some of the crime onto their poorer neighbors. The case against individual self-help, then, is not simply one predicated on the fraying of community. It is also based on the fact that private precautions cost money, and to expect those with less in society to bear a greater share of crime can offend notions of distributional justice.

But it does not follow that simply because individual self-help promotes atomization that a public enforcement solution is always appropriate. Instead, consider the power of community self-help. This power has been discussed obliquely in various literatures, perhaps most powerfully in Jane Jacobs' classic 1961 book.[4] Jacobs's goal was to investigate why crime rates differed among cities. She discarded the conventional theories of architecture and crime, such as those contending that building more public housing would prevent crime. Jacobs argued that if people could be brought out onto city streets, the crime rate would drop. She suggested, for example, that a house near a bar is much safer than one in a remote part of the countryside or city.[5] The bar attracts crowds whose presence and powers of observation may deter crime and draw attention, inducing those shopkeepers and residents who live nearby to watch the activity on the street more often. The bar also has a strong profit incentive to make sure that the area is safe for its customers, and the possibility of encounters between perpetrators and members of the general public may create enough uncertainty to make planning of crimes difficult.[6]

Jacobs' point was that communities play a crucial role in preventing crime. Yet much legal scholarship focuses on entities of the state or individuals, forgetting that

> the public peace—the sidewalk and street peace—of cities is not kept primarily by the police, necessary as police are. It is kept primarily by an intricate, almost unconscious, network of voluntary controls and standards among the people themselves, and enforced by the people themselves. In some city areas—older public housing projects and streets with very high population turnover are often conspicuous examples—the keeping of public sidewalk law and order is left almost entirely to the police and special guards. Such places are jungles. No amount of police can enforce civilization where the normal, casual enforcement of it has broken down.[7]

---

[4] JANE JACOBS, THE DEATH AND LIFE OF GREAT AMERICAN CITIES (1961). See also Neal Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039 (2002) (discussing Jacobs).

[5] JACOBS, *supra* note 4, at 37. *But see* M. RAMSAY, CITY-CENTRE CRIME 25-26 (Home Office, Research and Planning Unit Paper No. 10, 1982) (arguing that pubs can increase crime rates); Dennis W. Roncek & Ralph Bell, *Bars, Blocks, and Crimes*, 11 J. ENVTL. SYS. 35, 44 (1981) (finding that each additional bar on a residential block is correlated, on average, with four additional crimes on that block).

[6] JACOBS, *supra* note 4, at 54; *see also* FLOYD J. FOWLER, JR. ET AL., REDUCING RESIDENTIAL CRIME AND FEAR: THE HARTFORD NEIGHBORHOOD CRIME PREVENTION PROGRAM 2 (1979) ("Neighborhoods in which residents are out-of-doors, where surveillance is easy . . . are less attractive to offenders."); Robert Hanna, *Awareness*, *in* HANDBOOK OF LOSS PREVENTION AND CRIME PREVENTION 88 (Lawrence J. Fennelly ed., 3rd ed. 1996) (explaining that "watchers" can reduce crime).
Jacobs's observation is one instance of the great sociologist Erving Goffman's more general point that order can be created out of temporary and spontaneous social interactions. ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES 4, 8, 243-46 (1963); ERVING GOFFMAN, INTERACTION RITUAL 1-3 (1967).

[7] JACOBS, *supra* note 4, at 31-32.

Jacobs' work suggests that there may be significant payoffs to incorporating strategies that draw on the reservoir of the community. Instead of simply throwing more money at law enforcement, the self-help theorists are right to point out that there are advantages to private regimes.

But Jacobs' emphasis on the community reminds us that there are often costs to the community from individual self-help, even to crime rates. When cheap wire fences are placed around crime-ridden areas, iron bars on windows become pervasive, and "the Club" is ubiquitous, serious negative externalities can emerge, particularly the crippling of interconnectivity and the destruction of reciprocity.[8] A private precaution may help the individual user, but it expresses a view of fear and reflects attitudes that lawlessness has become pervasive. Bars on windows and other target hardening scares people away, fragmenting the community and the development of an ethos that promotes order. Thus, instead of decreasing crime, these acts of self-help can actually increase it.[9] Viewed this way, gated communities are by-products of public disregard of architecture, not a sustainable solution to crime.[10]

---

8 *See* Katyal, *supra* note 4, at 1067-71.

9 *Id.* at 1084-86.

10 Gated communities generally work along only one architectural precept, reducing access. They tend to have minimal natural surveillance and poor opportunities for social interaction, thereby creating a false sense of security. See Katyal, supra note 4, at 1085 n.172; Georjeanna Wilson-Doenges, An Exploration of Sense *of Community and Fear of Crime in Gated Communities*, 32 ENV'T & BEHAV. 597, 600, 608 (2000); *see also id.* at 605 (summarizing an empirical study showing that the sense of community in gated communities is lower); Edward J. Blakely & Mary Gail Snyder, *Divided We Fall: Gated and Walled Communities in the United States*, *in* ARCHITECTURE OF FEAR, at 85, 97 (Nan Ellin ed., 1997) ("[W]alls, street patterns and barricades that separate people from one another reduce the potential for people to understand one another and commit themselves to any common or collective purpose . . . ."); Udo Greinacher, *Fear and Dreaming in the American City*, *in* ARCHITECTURE OF FEAR, *supra*, at 288-89 ("Gated enclaves tend to be nothing more than an assemblage of individuals lacking any communal spirit. . . . [S]tudies conducted by police departments have failed to indicate a decline in property crime due to such elaborate and expensive measures.")

In addition, the social meaning of a gated community is one of fear—one that reinforces a view of crime as prevalent rather than controlled. *See* EDWARD J. BLAKELY & MARY GAIL SNYDER, FORTRESS AMERICA (1997) ("[G]ated areas . . . represen[t] a concrete metaphor for the closing of the gates against immigrants and minorities and the poverty, crime, and social instabilities in society at large."). Indeed, gated communities can attract criminals instead of repel them. *See* John Allman et al., *Sense of Security Can Be an Illusion*, SUN-SENTINEL, Feb. 25, 2001, at A1 (quoting police detective Mike Reed as saying that "some criminals think if it's a gated community, there must be something in there worth getting"). As a result of these factors, empirical studies have found that gated communities do not decrease crime. *See id.* (discussing a study of fourteen gated and fourteen nongated communities); Wilson-Doenges, *supra*, at 606 (discussing a more in-depth study of two communities); Nan Ellin, *Shelter from the Storm or Form Follows Fear and Vice Versa*, *in* ARCHITECTURE OF FEAR, *supra*, at 13, 42 (arguing that studies show that gated communities do not decrease crime); Jim Carlton, *Behind the Gate*, L.A. TIMES, Oct. 8, 1989, at 3 (describing police department studies in Irvine and Newport Beach, California, that find no reduction in crime).

In all of these cases, the public expression of fear cues additional crime, whereby norms of reciprocity have broken down and one cannot trust her neighbor. Not only does this breakdown weaken the public norm against crime in the area, it also means that those who have a greater propensity to follow the law will move out of such a neighborhood (or never move in the first place).[11]

Weak solutions to crime, whether through law enforcement or other means, stimulate these pernicious methods of self-help. A central goal of crime control strategies must be to provide a backdrop of security so that individuals do not have to resort to their own clumsy patches to the system. While this view has had little resonance in America, it has actually taken hold in Britain, where its Home Office has an entire team devoted to community self-help.[12] The British model is grounded in the promotion of networks, as the opening lines of its project attest:

> Networks which link local residents to each other are critical to the effective functioning of communities and thus of society at large. . . . [They are] a way of influencing insensitive or recalcitrant authorities and service providers. And what makes these networks operate is mutual aid or self help.... The absence of such communities will make it more difficult to enforce laws about anti-social behaviour, vandalism or keeping the streets clean. . . . Social decay will go in step with physical decay. The area will become unpopular. People who can do so will start to leave. Eventually a point of no return may be reached. Community self-help is one of the key ways to deal with this vicious circle.[13]

The British experience has found marked power from community self help:

> The benefits to the community of self-help activities can be assessed objectively – we see an effect on the ability of the community to cope with such issues as drug abuse, school truancy and exclusion and health problems. We can also measure the economic value. . . Less easily measurable are the changes in attitude that self-help brings. Organising mutual support increases people's self-confidence and their belief that they can affect the circumstances of their own lives. It can also act as a stepping stone to more formal links with the wider society beyond the estate...Benefits can be seen also in what might be called 'community self-confidence.' . . .
>
> ....[P]eople coming together to tackle the problem can give residents control over their own fear of crime; for some residents it is this fear which is keeping them trapped in their own home. An increase in informal activity leads to more street life as people take part, and this in itself reduces fear.[14]

---

11 *See, e.g.*, JAMES Q. WILSON, THINKING ABOUT CRIME, ch. 2 (rev. ed. 1975) (arguing that when crime rates are high, law-abiders move out of neighborhoods).

12 *See* HOME OFFICE, REPORT OF THE POLICY ACTION TEAM ON COMMUNITY SELF-HELP (1999).

13 *Id.* at 1.

14 HOME OFFICE, *supra* note 12, at 11, 14.

The Home Office report usefully begins the discussion of how some forms of individual self-help, such as staying indoors due to fear, fray the network. But self-help, through acts of vigilantism and the like, can cause active harm as well. The power of community self-help lies in its ability to minimize the active and passive harms to networks (that are present in the individual self-help variant) while simultaneously capturing the efficiencies of private solutions.

B. *In Cyberspace*

The uses of private precaution identified above have analogies in cyberspace. Consider, for example, a recent leading story in the *New York Times*, headlined "*Frontier Justice: On the Web, Vengeance is Mine (and Mine)*," evoking the vigilante tradition. The article explained how "[s]elf-appointed sheriffs scan eBay and Yahoo auctions looking for fraud. When they find it—or at least when they *think* they've found it—they warn buyers or make outrageously high bids themselves in order to end the auction."[15] The article provided numerous examples of such activity in other areas, concluding that cyberspace "is teeming with vigilantes who take matters into their own hands."[16]

There are any number of circumstances like the Yahoo! Auction example in which a weak solution to cybercrime will prompt greater forms of self-help. As Mitch Kapor puts it, "Vigilantes are in many cases responses to real problems where you'd like to see a much stronger institutional response—where there has been an institutional failure."[17] The impetus for self-help will arise even when a crime does little apparent damage. This is why the staple of cyberspace mavens -- that many computer crimes are ones of "curiosity" with "no real harm" – is wrong.[18] Crimes of curiosity can spur dangerous forms of self-help. The upshot of these computer intrusions is to raise the fear of using computers for sensitive transactions – whether it be credit card purchases, love letters, or sensitive business information. The teenager is punished not for what he did to the individual victim as much as what he has done to deplete the reservoir of trust among computer users. When crimes target that trust, the result can be to prevent people

---

[15] John Schwartz, *Frontier Justice: On the Web, Vengeance is Mine (and Mine)*, N.Y. TIMES, Mar. 28, 2004, at Sec. 4, 1.

[16] *Id.*

[17] *Id.*

[18] The defense here, as one hacker put it, is that the act "is just harmless exploration. It's not a violent act or a destructive act. It's nothing." Interview with Anonymous Juvenile Hacker who Pled Guilty to Breaking into NASA, available at http://www.pbs.org /wgbh/pages/frontline/shows /hackers/interviews/anon.html. The identity of this person was later revealed to be Jonathan James. *See Teen Gets a Six-Month Jail Term for Hacking*, Augusta Chron., Sept. 23, 2000, available at http://www.augustachronicle.com/stories/092300/tec_LA0666-2.001.shtml.

from coming onto the net and to prevent those that do from sharing information. This is the selfishness of self-help. As one researcher put it:

> During the Internet worm attack I experienced problems in my research collaboration with U.S. colleagues when they suddenly stopped answering my messages. The only way to have a truly international research community is for network communication to be reliable. If it is not, then scientists will tend to stick to cooperating with people in their local community even more than they do now.[19]

Under a self-help regime, therefore, the internet could begin to resemble that British community described by the Home Office where people stay indoors because they are afraid of crime.[20] The Net could fragment into a series of trusted networks for privileged users.[21] Individual sites, particularly new ones, would not let users access their information without adequate assurance that they will refrain from hacking and stealing private information. Accordingly, site managers would insist on high assurances that a person accessing a site is legitimate and will deny entry to those whose provenance is questionable. Unlike commercial establishments in realspace, web sites need not open their doors to anyone. The lack of regulation and due process characterize these transactions. The marginal benefit from one extra customer of dubious origin is exceeded by the damage a cyberthief can do to the site. (In realspace, a similar phenomenon occurs, regrettably along racial lines, when stores do not let "questionable" customers shop on their premises.) This can stymie development of the internet and make it difficult to secure the commercial and other advantages the technology promises to provide.

One of the great transformations in computing today is the emergence of "always on" networks at home and in the office.[22] These networks are a

---

[19] Jakob Nielsen, *Disrupting Communities*, in COMPUTERS UNDER ATTACK, at 524-25 (Peter J. Denning ed., 1990).

[20] *See* text at note 14, *supra*. The upshot of an over-reliance on victim precaution may be to return us to the age of the electronic bulletin board. When I was twelve years old, I used my Apple II to dial up various bulletin boards across the country and electronically chat with different users and swap programs. At no time would a board have more than ten people on it, and rarely would any one board have more than a few files of interest. No board was linked to the next one and there was no way of searching the individual boards to know who or what was on the others. With the connectivity of the internet, however, these problems have dissolved. Instead of isolated enclaves, web sites on the internet are linked together in ways that encourage users and programs to work together. The countless hours spent dialing and searching each board seriatim are over. Victim precaution can undermine this trend and force technology to spiral backwards.

[21] For a description of trusted networks, see Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us To Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137, 139-44 (1997).

[22] Approximately 50 percent of homes in the United States with Internet connections are expected to be using broadband very shortly. There has been a 60-percent growth rate in US broadband use during the past year, with half of that growth taking place since November 2003. Broadband Finally

promising means of increasing communication and connectivity between users, and can facilitate the instantaneous transfer and use of data.[23] But as incidence of computer intrusion mount, individuals will fear that their "always on" connection will increase the chance of an intruder reaching into their system. The occurrence of crime will induce users to structure their computer use in ways to minimize the harm, and one way to minimize the harm is to turn the computer off.

Put differently, the individual user contributes to a public good when her computer is on and she makes some of her data accessible via the Net. One reason for the startling number of such contributions has to do with the low costs of being public-minded – there are very few additional costs involved when someone uses their computer to publish items on the web. It is not simply publishing material – but even the raw processing power a computer has – that constitutes a public good. As Yochai Benkler has shown, thousands of individuals are making their computers accessible to take advantage of their distributed computing power to solve complicated tasks – such as finding the next prime number.[24] Large numbers of people today can and do publish information as well as donate their computers' processing power at little cost to themselves. But as the risks of privacy crime increase, those low costs suddenly balloon. Now the individual has to fear the consequences for her other, private, data once the computer is connected to the outside world. In this way, a crime can have effects that ripple far beyond the initial victim, striking fear in the universe of users more generally.

The impact of a hacker's activity therefore is subtle, and many times will take the form of stifling of network connections in the future. The Internet is the paradigmatic sphere in which the positive advantage of "network effects" is central – that the greater the size of the network, the greater the benefits.[25] The stifling of network connections thus can have dramatic negative consequences.

Dominates the United States, Broadband Business Forecast (May 4, 2004). Worldwide broadband installations number 100.8 million as of December 2003, a rise of 62.8 percent from the previous year. DSL Dominates as World Broadband Hits the 100-Million Mark, Broadband Business Forecast (April 6, 2004).

[23] For a discussion of broadband's societal benefits, see Office of Technology Policy, U.S. Dept. of Commerce, *Understanding Broadband Demand: A Review of Critical Issues* (Sept. 23, 2002) ("Broadband is an incredible *enabling* technology. It allows businesses that are willing to embrace Internet business solutions to transform business processes and realize significant returns on investment. It offers consumers new opportunities to work or learn more productively (at their desks or from home), publish multimedia, switch from viewers of entertainment to participants, and – most importantly – dramatically expand their communication possibilities.").

[24] See Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 384-85, 429-36 (2002).

[25] A network effect occurs when the utility of a good increases with the number of other agents who are consuming the same good. Michael L. Katz & Carl Shapiro, *Network Externalities, Competi-*

But the self-help proponents can say, with some justification, just what the police said about car theft above. There are any number of ways to prevent hacking, they could point out, including firewalls and disconnecting computers from open networks. If only encryption, firewalls, remote servers, intrusion-detection systems, and other forms of technology were pervasive, the tempting argument goes, the community harms from crime would cease to exist.

It is worth pointing out at the outset that, even if adopted, these technological countermeasures amount to a dead-weight loss, a consequence of the crime that supposedly had "no real harm." And many times the countermeasures impose real harm to their adopters. "[M]ost organizations don't spend a lot of money on network security. Why? Because the costs are significant: time, expense, reduced functionality, frustrated end users....The same economic reasoning explains why software vendors do not spend a lot of effort securing their products. The costs of adding good security are significant—large expenses, reduced functionality, delayed product releases, annoyed users—while the costs of ignoring security are minor: occasional bad press, and maybe some users switching to competitors' products."[26] The difficulties with self-protection may explain why a study of more than 2000 computer users recently found that 20% of them failed to perform any routine cyber hygiene at all and that 40% said they had not taken steps to prevent the Blaster worm.[27]

In any event, some private precautions will be able to be adopted without a great loss in connectivity because they resemble a simple door lock more than they do a fortress.[28] Yet even these systems are likely to be adopted disproportionately, and with severe distributional consequences to boot. If law enforcement did not police cybercrime, so that the burden of fending off attacks were left to individual victims, only the better off may

---

tion, and Compatibility, 75 AM. ECON. REV. 424, 424 (1985); *see also* Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, J. ECON. PERSP., Spring 1994, at 93, 94 ("Because the value of membership [in a network] to one user is positively affected when another user joins and enlarges the network, such markets are said to exhibit 'network effects,' or 'network externalities.'"); S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, J. ECON. PERSP., Spring 1994, at 133 (refining and limiting the Katz and Shapiro concept).

[26] Bruce Schneier, Computer Security: It's the Economics, Stupid, First Workshop on Economics and Security, Berkeley, May 2002, at 1.

[27] Information Technology Association of America, Press Release, Aug. 21, 2003.

[28] Technical solutions may fail for other reasons, such as the fact that some forms of computer crime are not amenable to them. Not only does the march of technology work to benefit criminals as well as noncriminals, thereby conferring ever greater intrusion prowess, it is often times impossible to build fully secure systems against intrusion. Encryption may work between two users, but it can't stop keystroke loggers and intrusion methods that capture screen images. Electronic detection systems are always susceptible to a criminal masquerading as an authorized user. Just as architecture in realspace cannot eliminate crime altogether without massive other costs, so, too, in cyberspace.

be able to thwart the attacks, leaving the rest of the computer-using population vulnerable.

Any calculation of optimal victim precaution must therefore take into account the harms imposed by such precaution. It is dangerous to expect individual victims to do too much. And yet much legal scholarship simply assumes away the problem. Consider torts. The famous Learned Hand Test states that negligence depends on whether the burden of private precautions exceeds that of the probability of an accident multiplied by the harm of that injury.[29] In the case that gave rise to the test, a ship had broken away from its tow and smashed into a tanker. The ship owner sued the towing company, but the towing company said that the ship owner was contributorily negligent for not having an attendant on board. Hand sided with the towing company, stating that the ship owner could have avoided the accident by having placed an attendant on board.[30] Hand, however, trained his eye only on the cost of precautions to the ship owner. While this limited focus may have been appropriate on the facts of that case, the general formula needs revision.

When private precautions impose negative externalities (in that they cause harm that is not borne exclusively by the precautionary party), the Hand test will lead to a suboptimal result. Focusing only on the victim's costs, without due regard for the cost of the precautions to society, can skew reasoning. Computer crime is a nice illustration of the point. If victims build firewalls that are too strong, collective benefits will be undermined. As the Cornell Commission Report on the Morris worm case states, a "community of scholars should not have to build walls as high as the sky to protect a reasonable expectation of privacy, particularly when such walls will equally impede the free flow of information."[31]

Forcing individuals to bear the cost of computer crime will promote sales of anti-virus software, intrusion systems, and the like. Yet the ability to afford, and the knowledge to use, such technologies will not be distributed equally. Those with fewer resources will not be able to adopt them in the same way that richer individuals and institutions can. Because these methods are often technical, moreover, there will be some who have the resources, but lack the skills necessary to use the technology effectively.

The distributional consequences of this drift toward private precautions can be devastating. Already, users of America Online, a group that tends toward less technical sophistication, are being inundated with spam in ways that other users are not. As the technical capacities of computer criminals grow, unacceptable danger lurks to less sophisticated and poorer users. The result will be a less private, more vulnerable, Internet experi-

---

29 United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

30 *Id.* at 174.

31 Ted Eisenberg et al., *The Cornell Commission: On Morris and the Worm, in* COMPUTERS UNDER ATTACK: INTRUDERS, WORMS, AND VIRUSES, at 258 (Peter J. Denning ed., 1990).

ence for these groups, and this may drive some off the Net altogether, and leave others afraid to have as public a presence on the Net.

It is tempting to think that technology can solve this problem, too. After all, many of the devices that protect against computer crime are simply pieces of software – antivirus programs, some firewalls, and the like. Because additional software units can be manufactured at low marginal cost, the argument goes, the distributional divide will not occur; richer users will pay for a product's research and development and in turn such payments will subsidize use by the relatively poorer. But it is dubious to think that the manufacturers of these products would cut their costs enough so that their more sophisticated systems would be cheaply available. (Anyone who doubts this should take a look at the pharmaceutical industry.) And even if they did, the upshot could be to diminish cybersecurity overall. If the great majority of computer users adopted the same firewall and antivirus systems, danger of a different kind would lurk: the lack of diversity. Indeed, it may be that richer computer users have adverse interests to poorer ones – they do not want the protection software they use to be widely implemented – for if it were, their security may suffer. Greater prevalence may make their program not only a more prominent, but also a more inviting, target.

II. THE COMMUNITY SELF-HELP MODEL

A. *In Realspace*

There is a growing movement towards community justice based on the notion that the governments cannot adequately solve criminal problems on their own. Community policing refers to techniques of law enforcement that locate police directly in communities, where they are responsive to local concerns and pursue local agendas. The idea is to prosecute those cases that the community feels deserve sanction, instead of relying on standardized instructions from a centralized headquarters.[32] When done correctly, community policing brings more people out onto the streets where they can perform their natural surveillance role. And community ap-

---

[32] Consider the following:

- Police are working as partners with residents in communities to identify the problems that concern them the most.
- Prosecutors are moving their offices into local areas and talking to residents to better respond to their concerns.
- Corrections officers are working with communities to discuss ways to rehabilitate offenders who have recently been released from imprisonment.

David R. Karp & Todd R. Clear, *Community Justice: A Conceptual Framework*, *in* 2 CRIMINAL JUSTICE 2000: BOUNDARY CHANGES IN CRIMINAL JUSTICE ORGANIZATIONS 323 (Charles M. Friel ed., 2000), *available at* http://www.ncjrs.org/criminal_justice2000/vol_2/02i2.pdf.

proaches today are starting to move into the phase of crime prevention, and not just crime prosecution.[33]

The advantages of this approach are many, but two are salient for our purposes. First, a main drawback of conventional policing, as the individual-self-help proponents have observed, is that it trades off with private methods of controlling and reacting to crime. Community-based solutions sidestep this by incorporating private actors directly into the process of controlling crime. As such, the signal is sent that crime prevention depends not only on the government, but also on the community. Put differently, community strategies emphasize *stewardship*, in that it "calls on citizens to view themselves as responsible for the welfare of the larger community."[34]

Second, community-based solutions do a better job of promoting values of order and safety than the public model. When law enforcement is solely responsible for policing, a backlash can develop among residents. Such "top-down" solutions are not particularly effective ways of generating order norms. Instead, "[w]hen a community responds to a criminal incident, it seeks not merely to restore credibility to the community's conception of the moral order...but also to symbolically affirm community norms for others who have not disobeyed them."[35]

That is the story of community self-help vis-à-vis law enforcement, yet it also has a set of advantages over its individual variant. Individualized self-help and conventional policing, after all, both adopt a "'we-they' syndrome"[36] that announces an atomized view of crime prevention. In this model, "someone else" takes care of the problem (or does not). Such a model fails to foster a set of community values and norms, and it does not generate the type of inclusiveness celebrated, for example, in the British report on community self-help.

Finally, there are other payoffs to community self-help. One of the most dangerous problems with criminal enforcement, as I argued in *Deterrence's Difficulty*, is substitution effects.[37] Just as a high price on a product like coffee can induce consumers to switch to tea, a high criminal sanction on one activity can prompt them to substitute something else. But sometimes the government gets the penalties wrong – and encourages substitution to criminal offenses that produce more harm. One example might be crack cocaine, for there is some data showing that the harsh penalties on crack enacted by Congress in 1986 prompted dealers to shift to carrying heroin (the punishment ratio was approximately 200:1). Another form of substitution is more obvious – geographic substitution – whereby a crackdown in one area of a city induces the criminals to move to another area.

---

33 *Id.* at 348.

34 *Id.* at 337.

35 *Id.* at 331.

36 *Id.* at 326.

37 Neal Kumar Katyal, *Deterrence's Difficulty*, 95 MICH. L. REV. 2385 (1997).

There are good reasons to think that, in different instances, residents in a community and law enforcement will have private information that may be relevant to avoiding substitution effects. For example, residents may be aware of new locations for crime breaking due to geographic substitution. And law enforcement might have knowledge about why a particular law might engender perverse substitution effects, like the heroin/crack one, and want to steer private self-help measures away from enforcing crack-cocaine punishments. In this way, dialogue between both sides may yield a more optimal policy.

Of course, community-self help can also cause problems of its own. The most pernicious is the well-known tendency of groups to take extreme positions. A wide body of psychological research over the last century reveals that people tend to act differently in groups than they do as individuals.[38] Some of the work is tentative, thereby precluding robust results. Nevertheless, it is generally accepted that groups are more likely to polarize towards extremes, to take courses of action that advance the interests of the group even in the face of personal doubts, and to act with greater loyalty to each other.[39] Much of the most influential research focuses on how group membership changes an individual's personal identity to produce a new *social identity.* Muzafer Sherif's 1936 experiments, for example, showed that people estimating how far a pinpoint of light moved in a dark room tended to conform to what others in the room said. Even a wildly off-base group member would influence the results. Follow-up studies confirmed that individuals would internalize the views of others and adhere to them even a year later.[40]

---

[38] John C. Turner, *Foreword* to S. ALEXANDER HASLAM, PSYCHOLOGY IN ORGANIZATIONS: THE SOCIAL IDENTITY APPROACH xi (2001) ("Moving from the 'I' to the 'we' psychologically transforms people and brings into play new processes that could not otherwise exist. Indeed it is to this creative capacity that most organizations owe their success."); *see also* HASLAM, *supra*, at 26 ("groups *change* individuals and this in turn makes groups and organizations more than mere aggregations of their individual inputs"); Margaret Wetherell, *Group Conflict and the Social Psychology of Racism, in* IDENTITIES, GROUPS, AND SOCIAL ISSUES 175, 203 (Margaret Wetherell ed., 1996) ("group membership *in itself* has profound effects upon the psychology of the individual, regardless of personality and individual differences").

[39] The research responsible for these conclusions spans the range of traditions in psychology. *See, e.g.*, Sigmund Freud, *Group Psychology and the Analysis of the Ego, in* 18 THE STANDARD EDITION OF THE COMPLETE PSYCHOLOGICAL WORKS OF SIGMUND FREUD 65, 72-73 (James Strachey trans., 1955) (quoting Le Bon's claim that "the fact that [individuals] have been transformed into a group puts them in possession of a sort of collective mind which makes them feel, think, and act in a manner quite different from that in which each individual of them would feel, think, and act were he in a state of isolation . . . exactly as the cells which constitute a living body form by their reunion a new being which displays characteristics very different from those possessed by each of the cells singly."); *see also* George A. Akerlof & Rachel E. Kranton, *Economics and Identity*, 115 Q.J.ECON. 715 (2000).

[40] These experiments are described in detail in LEE ROSS & RICHARD E. NISBETT, THE PERSON AND THE SITUATION 28-31 (1991) and ROGER BROWN, SOCIAL PSYCHOLOGY (2d ed. 1986).

For our purposes, perhaps the most important finding is that groups are more likely to have extreme attitudes and behavior. This research began with findings showing "risky shifts"—predictability in the conformity result in that people take greater risks in groups.[41] Subsequent work found that the phenomenon was not limited to shifts in risk, and that groups polarize in the direction their members were already tending.[42] For example, French students who already liked De Gaulle liked him even more after discussing him in a group, and those that did not like Americans liked them even less after discussing Americans in a group.[43]

This literature could be read to predict that community self-help might exacerbate the problems of vigilantism instead of mitigating them. There is some evidence that supports this view. For example, in the 1980s the police launched an operation in downtown New Haven targeted at prostitution. The result, as substitution theory would predict, is that many of the prostitutes just moved elsewhere, to another location a few blocks away in Edgewood Park. But some residents of Edgewood grew concerned with the dangers brought by the new arrivals, and took action. They began writing down license plate numbers of the "johns," looking them up through Department of Motor Vehicle registrations, and started aggressively posting "john of the week" fliers that had the john's name, address, and phone number.[44] There are reports of other, far more frightening, examples, such as citizen patrols that single out people on the basis of race.[45]

Yet these group dynamics actually underscore why the government should do more to encourage community self-help. By expanding the circle

---

[41] J. A. Stoner, A Comparison of Individual and Group Dimensions Involving Risk (1961) (unpublished master's thesis, Massachusetts Institute of Technology, School of Industrial Management). For further descriptions readers should consult HASLAM, *supra* note 38, at 153-73; Kenneth L. Bettenhausen, *Five Years of Groups Research: What We Have Learned and What Needs To Be Addressed*, 17 J. MGMT. 345, 356-59 (1991); Noah E. Friedkin, *Choice Shift and Group Polarization*, 64 AM. SOC. REV. 856, 856-60 (1999); Myers & Lamm, *The Group Polarization Phenomenon*, 83 PSYCHOL. BULL. 602, 606-10 (1976); Charles Pavitt, *Another View of Group Polarizing: The "Reasons for" One-Sided Oral Argumentation*, 21 COMM. RES. 625, 625-29 (1994); Cass R. Sunstein, *Deliberative Trouble?: Why Groups Go to Extremes*, 110 YALE L.J. 71 (2000).

[42] *See* Markus Brauer et al., *The Effects of Repeated Expressions on Attitude Polarization During Group Discussions*, 68 J. PERSONALITY & SOC. PSYCHOL. 1014, 1015 (1995) (describing polarization); JOHN C. TURNER ET AL., REDISCOVERING THE SOCIAL GROUP 142 (1987) ("[L]ike polarized molecules, group members become even more aligned in the direction they were already tending."); Myers & Lamm, *supra* note 41, at 603 (providing similar account). Polarization therefore runs against the finding by cognitive psychologists that individuals avoid extreme positions. *See* Katyal, *supra* note 37, at 2364-65 (discussing studies).

[43] Serge Moscovici & Marisa Zavalloni, *The Group as a Polarizer of Attitudes*, 12 J. PERSONALITY & SOC. PSYCHOL. 125 (1969).

[44] Karp & Clear, *supra* note 32, at 355-56.

[45] Alison Mitchell, *In an Often Violent City, a Not-so Simple Beating*, N.Y. TIMES, Dec. 6, 1992, § 1, at 51; *see also* Wesley Skogan, *Community Organizations and Crime, in* CRIME & JUSTICE: A REVIEW OF RESEARCH (Tonry & Morris eds., 1988).

of individuals who are responsible for crime prevention, community strategies can break down destructive group dynamics. After all, it is fairly obvious that proposals for "individual" self-help are not typically calls for strategies that are implemented by lone actors. Some will require the assistance of a few like-minded individuals. Those individuals are most likely to be the direct victims of crime. In such settings, group identity and inclusiveness can become pernicious. The point of this paper is to advocate for strategies that expand the size of the group, and by so doing, minimize some of the destructive force of small groups.[46] Think of it as Madison's Federalist 10 as applied to self-help. By expanding the size of the group, networks begin to form and extremism can be reduced. Government incentives for self-help, to the extent they are available, should therefore carefully reflect on the benefits of group strategies and target opportunities there.

B. *In Cyberspace*

At the outset, it is worth raising the question of whether realspace community self-help can be a template for much in cyberspace, since the realspace concept is built on local geographies. As the British Home Office puts it, "The notion of place is, self-evidently, central to community self-help. . . . 'Give where you live' is an appropriate slogan for any campaign to promote it."[47] The fact that there is no single geographic "place" in cyberspace might therefore be thought to preclude the notion of community self-help. But the fact that "place" is unfettered online cuts both ways, since it means that opportunities for self-help expand, too. The community in cyberspace may revolve around any number of things, such as a virtual place (eBay); a place in realspace (Georgetown); a concept (Maoism); or even a sport (windsurfing). The proliferation of such communities, and the ease of transacting in each one, suggest robust potential for community solutions.

The methods of employing community self-help methods in cyberspace are often intensely practical, and many already exist, such as the exchange of best practices regarding cybersecurity. These methods largely replicate neighborhood crime prevention exchanges in realspace. Other solutions, however, are more exotic, such as reputational mechanisms that assess the trustworthiness of individuals in a decentralized fashion and

---

[46] Several studies have found that increasing group size can reduce the social identity of the group. *See* David Canter, *Destructive Organizational Psychology*, *in* THE SOCIAL PSYCHOLOGY OF CRIME: GROUPS, TEAMS, AND NETWORKS 323, 327 (David Canter & Laurence Alison eds., 2000); Roderick M. Kramer, *Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions*, 50 ANN. REV. PSYCHOL. 569, 585 (1999).

[47] HOME OFFICE, *supra* note 12, at 26.

peer-to-peer surveillance. These methods will be taken up in the next section, after a brief explanation of why community self-help is necessary at all.

It turns out to be very difficult to catch cybercriminals. The cost of government identification, investigation, and prosecution of cybercrime is too great. Despite some indications of the government's ability to trace criminal suspects online,[48] the truth is that tracing is very difficult. A criminal may leave behind a trail of electronic footprints, but the footprints often end with a pseudonymous e-mail address from an ISP that possesses no subscriber information. Moreover, finding the footprints is often very difficult. Criminals can be sophisticated at weaving their footprints through computers based in several countries, which makes getting permission for real-time tracing very difficult.[49] Unlike a criminal who needs to escape down a particular road, a criminal in cyberspace could be on any road, and these roads are not linked together in any meaningful fashion due to the routing of individual packets.

Implementing a tracing order can be difficult; since the breakup of AT&T, long distance-calls and data transmissions are often handled by several entities. These entities might even be based in other countries, depending on the location of the perpetrator and on whether or not weaving is being used. (The foreign location gives rise to a number of constitutional and statutory questions in each country about whether the transmission can be traced.) By the time the relevant authorities grant their permission, the trail may be cold, as ISPs and other entities may have deleted the information necessary to perform the trace. Furthermore, curious administrators and company officials may damage the trail by poking around.[50] Even if the transmission can be traced quickly before it is damaged, the trace may dead-end into a cell phone line. As cellular phones become commonplace, tracing has become even harder because criminals view cellular phones as "disposable" and treat them like one-time pads to be discarded after use. In addition, the technology to fake cell phone locations and identities is be-

---

48 *See Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology), 2000 WL 249419.

49 *Cybercrime: Hearing Before the Subcomm. on Commerce, Justice, and State, the Judiciary, and Related Agencies of the S. Appropriations Comm.*, 106th Cong. 20 (2000) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

50 *Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of "Mudge," Vice President of Research and Development, @Stake, Inc.) ("People implicitly know that they should not wander around a crime scene disturbing potential evidence. Further, when called in to look at a crime scene the investigators will restrict access . . . . Unfortunately, it is still the exception when dealing with filesystems and transient data found on computers and networks."), 2000 WL 232400.

coming widespread.[51] And even if calls can be traced to a computer in a hard location, there is no guarantee that the user of the computer is present.[52]

For these reasons, community self-help strategies offer a promising method of crime prevention to stop cybercrime before prosecution becomes necessary. This section will first discuss information-promotion strategies and will then take up more novel strategies based on peer-to-peer concepts.

1. Information Promotion

Best practices. A key type of community self-help is for corporations to share best practices regarding cybersecurity with each other. The federal government has taken some small steps to encourage private firms to share information about cybersecurity among themselves. President Clinton's PDD-63 had, as one of its aims, facilitating this private information sharing.[53] The Bush Administration's *National Strategy to Security Cyberspace* also has made some steps in this regard.[54] The government has also urged small business to join information-gathering organizations like the ISAlliance.[55] Some private entities have started to cooperate, prodded by these efforts. For example, an industry-led coalition of security experts called the Awareness and Outreach Task Force has proposed a forum series, in which the Department of Homeland Security would bring CEOs of large enterprises together for conversations and information exchanges regarding cy-

---

[51] U.S. Dep't of Justice, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET: A REPORT OF THE PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET 11 (2000), *available at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm, at 28-31. The head of the DOJ's Criminal Division has similarly stated:

> While less sophisticated cybercriminals may leave electronic "fingerprints," more experienced criminals know how to conceal their tracks in cyberspace. With the deployment of "anonymizer" software, it is increasingly difficult and sometimes impossible to trace cybercriminals. At the same time, other services available in some countries, such as pre-paid calling cards, lend themselves to anonymous communications.

James K. Robinson, Internet as the Scene of Crime, Remarks at the International Computer Crime Conference (May 29-31, 2000), *at* http://www.usdoj.gov/criminal/cybercrime/roboslo.htm.

[52] In the Philippines ILoveYou investigation, for example, police readily traced calls to an apartment in Manila, but the user that launched the virus attack was not apparent. *See* D. Ian Hopper & Reuters Wire Service, *Authorities Seek to Question Pair in "Love Bug" Attack* (May 11, 2000), *at* http://archives.cnn.com/2000/ASIANOW/southeast/05/11/ilove.you/index.html ("[Authorities] noted, however, that anyone who had access to the apartment and the computer could have created the virus.").

[53] The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (1998), *available at* http://www.mipt.org/pdf/ClintonPolicyCIP_PDD63.pdf.

[54] *The National Strategy to Security Cyberspace*, *supra* note 1, at 37 (2003).

[55] *See* INTERNET SECURITY ALLIANCE, COMMON SENSE GUIDE TO CYBER SECURITY FOR SMALL BUSINESSES (2004) (advising small business about how to secure their systems, including joining information gather alliances), *at* http://www.us-cert.gov/reading_room/CSG-small-business.pdf.

bersecurity.[56] Such efforts, while by no means sexy (or, more precisely, just about as sexy as neighborhood watch), are the types of community-self help programs likely to make a real difference. Government, through ISACs and other mechanisms, can create a framework by which such information is exchanged.

Encouraging cooperation/Removing Barriers. Not only should our government foster community self-help, it should update its old laws that stymie these solutions. *The National Strategy to Security Cyberspace* urges companies to cooperate "[t]o the extent permitted by law," but in order to allow robust information sharing, the government may need to do what it did in the Year 2000 Information and Readiness Disclosure Act and exempt sharing of information about cybersecurity threats and best practices from antitrust laws.[57] For example, the Congress might reassess the apparently defunct Cyber Security Information Act of 2000 proposed by Republican Tom Davis and Democrat Jim Moran, which aimed to create such an anti-trust exemption.[58] Relaxing antitrust laws raises concerns about unfair competition, but a carefully tailored bill to permit only cybersecurity sharing might address these worries.

Viruses. Criminal prosecution here is costly and inefficient. Often times, viruses are best prevented through simple software, such as Symantec Anti-Virus, installed by individual users. Such solutions can have community aspects, in that the power of the software may derive from the creation of a virtual community. Members of that virtual community may be unconsciously or consciously reporting their experiences and prompting cures.[59] The anti-virus program/community is the beginning of what self-help to prevent viruses could look like. A more radical form of self-help is now appearing whereby individuals take it upon themselves to launch coun-

---

[56] *See* AWARENESS AND OUTREACH TASK FORCE, REPORT TO THE NATIONAL CYBER SECURITY PARTNERSHIP (2004), *available at* http://www.cyberpartnership.org/Aware_Report.pdf.

[57] For example, in 2000 the Department of Justice announced that it would not challenge the formation of the Electric Power Research Institute (EPRI), a non-profit organization of companies in the energy industry, which aimed to enhance information sharing about cyber threats. *See* Press Release, Department of Justice, Justice Department Approves Information Exchange Proposed by the Electric Power Research Institute (October 2, 2000), *available at* http://www.usdoj.gov/atr/public/press_releases/2000/6619.htm. This specialized exemption from anti-trust laws is a step in the right direction, but a more broad-based solution could do more to harness the private sector.

[58] H.R. 2435, 106th Cong. (2000); *see also* Letter from R. Bruce Josten, Executive Vice President, Government Affairs, U.S. Chamber of Commerce, to the U.S. House of Representatives in Support of the Cyber Security Research and Development Act (February 6, 2002) (supporting David and Moran's legislation because "under current law, businesses are often reluctant to share information with each other and with federal and state governments because of fears of potential antitrust liability and Freedom of Information Act (FOIA) disclosure of sensitive information.").

[59] For one example of a more exotic community based solution, involving a feedback system of individual users, see Marshall Jon Fisher, *Moldovascam.com*, ATLANTIC MONTHLY, Sept. 1997, at 19-22.

terstrikes against virus propagators. Those proposals will be discussed in Part III.

Honeypots and CyberWatch. Online communities are being formed to ferret out and learn about cybercriminals. One of the most promising methods involves honeypots, which essentially are decoy sites designed to look like promising targets to hackers. By luring potential hackers into the honeypot trap, its operators discover the attack techniques used in the operation and perhaps even uncover the IP address of the offender.[60] The Honeypot Project links together a number of honeypot operators to disseminate the information that each obtains.[61]

In a self-conscious analogue of realspace community prevention, Cyberangels calls itself "the first cyber-neighborhood watch and is one of the oldest in online safety education."[62] Cyberangels is a group of IT professionals and law enforcement officers who exchange ideas about cybercrime prevention. They also have a group of over 3,000 volunteers to patrol the internet for child molesters and child pornographers. The European Union recently adopted a plan that relied on similar ideas, suggesting that reporting of criminal acts by users would combat cybercrime: "An effective way to restrict circulation of illegal material is to set up a European network of centres (known as hot-lines) which allow users to report content which they come across in the course of their use of the Internet and which they consider to be illegal."[63]

Crime Impact Statements. The Crime Impact Statement, modeled after the Environmental Impact Statement required under federal law, is a realspace device that encourages developers to think about the consequences of their design on crime rates. The issuance of such statements can prompt community dialogue and deliberation by revealing private information to the public. Government could require companies that release major products, such as software platforms, to provide a similar impact statement. Statements could discuss some of the key security features of the software, such as its encryption and password protocols, certify that the trapdoors that programmers use to quickly make changes to the program have been removed, and explain how the program should be configured to prevent at-

---

[60] *See* Pia Landergren, *Hacker Vigilantes Strike Back* (June 20, 2001), *at* http://archives.cnn.com/2001/TECH/internet/06/20/hacker.vigilantes.idg/. *See generally* NANCY RADER, HONEYPOTS: SWEET AND STICKY FOR THE CYBER "BAD GUYS," *available at* http://www.giac.org/practical/GSEC/Nancy_Rader_GSEC.pdf (2003) (giving an overview and history of "honeypots" and how they operate).

[61] http://project.honeynet.org/ (last visited Nov. 20, 2004); RADER, *supra* note 60, at http://www.giac.org/practical/GSEC/Nancy_Rader_GSEC.pdf.

[62] http://www.cyberangels.org/ (last visited Nov. 20, 2004); http://www.usatoday.com/tech/columnist/cctam028.htm (last visited Nov. 20, 2004); http://www.cnn.com/2000/TECH/computing/06/16/cyberangels.idg/ (last visited Nov. 20, 2004).

[63] *Community Action Plan on Promoting Safer Use of the Internet*, 1999 O.J. (L 33) 1, 6, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/1999/l_033/l_03319990206en00010011.pdf.

tack. Requiring these statements by itself will make it more likely that developers will ship their software in secure default modes. Because an impact-statement requirement does not mandate any particular form of architectural design, it couples the flexibility of a market-based solution with the power of transparency. And it begins to stimulate a conversation among the community of product users about security.

Open Source. Consider the virtues of community self-help in the context of the raging debate about open-source software security. Open-source devotees claim that their programs are inherently more secure than closed-source ones by dint of the number of eyeballs testing the code.[64] This argument is almost always overstated. For certain forms of software that are highly specialized, it is not realistic to think that there will be citizen-activist eyeballs monitoring the code for flaws. Rather, openness in the code might reveal, disproportionately to closed code, security flaws that can be exploited.[65] But if a program is ubiquitous, like a computer operating system, the open-source proponents are right that the multitude of users will examine the code and reveal its flaws.

The point of the community-based model is to say that this debate over open-source misses another variable, stewardship. Open-source programs

---

[64] OPEN SOURCE INITIATIVE, OPEN SOURCE FAQ, *at* http://www.opensource.org/advocacy/faq.php (last visited Nov. 20, 2004) (arguing that closed sources "create a false sense of security"); Michael H. Warfield, *Musings on Open Source Security Models*, LINUXWORLD.COM (last visited Nov. 20, 2004) ("The closed source camp likes to point out every open source security advisory as evidence that open source is insecure. In doing so, they conveniently ignore the counter examples in their own advisories. They also conveniently overlook the fact that open source problems are often found and fixed before they're widely exploited, while some closed source problem go unaddressed for months, or longer."), *at* http://www.br.fgov.be/SCIENCE/INFORMATICS/doc/ramparts.html; ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR (2000) (making a similar argument for open source security), *available at* http://www.catb.org/~esr/writings/cathedral-bazaar/; Nicholas Petreley, *Microsoft's Road to Consumer Trust Is To Open Source Windows*, INFOWORLD (Nov. 13, 2000) ("If having the source code makes it easy to spot weaknesses, the best way to find and plug security holes is to make the source code as widely available as possible and solicit the input of those who use it."), *at* http://www.infoworld.com/articles/op/xml/00/11/13/001113oppetreley.xml; *and* BRIAN HATCH ET AL., HACKING LINUX EXPOSED: LINUX SECURITY SECRETS AND SOLUTIONS (2001) (similar).

While empirical data is limited, Microsoft's closed source web server, IIS, was the most frequently targeted web server for hacking attacks in 2001, despite the fact that there are a larger number of open source Apache systems in use. *See* DAVID A. WHEELER, WHY OPEN SOURCE SOFTWARE/FREE SOFTWARE (OSS/FS)? LOOK AT THE NUMBERS!, *at* http://www.dwheeler.com/oss_fs_why.html (last modified Nov. 7, 2004). Indeed, some firms are switching to Apache to avoid the viruses that attack Microsoft server software. *See* Rutrell Yasin, *So Many Patches, So Little Time*, INTERNETWEEK (Oct. 4, 2001) (explaining that after the Code Red virus, the law firm Fenwick & West switched to Apache), *at* http://www.internetweek.com/newslead01/lead100401.htm; Warfield, *supra* (discussing how an open source model quickly solved a problem with the PGP2.6 encryption program).

[65] *E.g.*, KENNETH BROWN, OPENING THE OPEN SOURCE DEBATE 8, *at* http://www.adti.net/opensource.pdf (2002) (arguing that opening the code teaches hackers how to attack it).

involve the user in the process of security, instead of relegating it to someone else. Closed-source software creates the same type of "we/they syndrome" as conventional policing does. There just is not much impetus to try to come up with solutions to Windows XP's security flaws when one cannot even access the code. The closure of the code sends a signal, and that signal is that Microsoft will take care of your security problems. Such centralized solutions are no doubt successful under certain conditions, but, as the self-help proponents rightly point out, they can also be inefficient. In this way, the Linux community, often viewed as a bunch of anti-market sympathizers, have much in common with the market-based economists who emphasize self-help on efficiency grounds. Centralized solutions may have inefficiencies of their own, and distributed security may be a better model at times.

2. Two Models of Community Self-Help through Peer-to-Peer Surveillance

One of the unforeseen advances in computer networking has been the emergence of peer-to-peer systems (p2p). In its most popular form—file sharing services such as KaZaA—p2p permits users to share content with one another without the use of a centralized server. The p2p model has the potential to revolutionize computing. Instead of everyone trying to access the CNN site at the same time, for example, a computer might simply "chain" CNN's content from another peer computer that has just visited the site. Search engines are made more efficient by using the power of multiple computers and aggregated searches.[66] Yet p2p applications require significant trust in one's peers, and fear of viruses, hacking, and other computer crimes have severely discouraged their use.[67]

Like open source and e2e, p2p is not necessarily good or bad in all contexts. Some have celebrated it explicitly, others implicitly.[68] And some have harshly attacked it.[69] At the application level, one deep question is

---

66 MICHAEL MILLER, DISCOVERING P2P 34-35, 194-203 (2001) (discussing search engines that use p2p technology).

67 Security is the Achilles heel of p2p. As even the strongest p2p admirers concede, "security remains the biggest question facing all peer-to-peer applications." HASSAN M. FATTAH, P2P: HOW PEER-TO-PEER TECHNOLOGY IS REVOLUTIONIZING THE WAY WE DO BUSINESS 180 (2002); *see also* MILLER, *supra* note 66, at 63-64 (discussing the impact of viruses on the Gnutella network).

68 FATTAH, *supra* note 67, at 12 (explaining how "Napster wasn't just about sharing music," but rather "about building empowered communities, about building an empowered workforce, and about mapping your computer systems to better match the behavior and quirks of people").

69 *See* Cory Doctorow, *Hollywood's Copyright Fight Might Hit Digitally Close to Home*, ORLANDO SENTINEL, Oct. 20, 2002, at G1 (discussing the "Hollywood call for a ban on P2P"); *Education Sector Wants Controllable Broadband*, BROADBAND BUS. REP., Oct. 8, 2002 (observing that "Indi-

whether p2p might provide a new security model. Already, p2p security applications are emerging, with companies such as McAfee using p2p to provide quick updates for its anti-virus software, thereby avoiding the peril of having millions of customers crash their servers looking for updates when new viruses hit the Net.[70] As Jane Jacobs might ask, could community-strategies enable peers to guarantee digital security instead of always relying on law enforcement or private self-help? Consider two possibilities.

Illuminating Cyberspace. Today cyberspace is *dark.* One cannot see what other users are doing at any given time. This makes real-time intervention by peers quite difficult. Certain forms of crime might be prevented in realtime, such as online harassment and stalking in chat rooms, but a large number of offenses (among them, unauthorized access and disruption, piracy, and child pornography) are not visible at all to peers. But, as concern about computer crime becomes greater, the architecture could flip—just as it did with the advent of gas lighting and electricity—and shed light on users in cyberspace. Imagine that each ISP customer, on a monthly basis, is randomly aggregated with forty-nine other customers. Each customer, or their pseudonym, would show up as a small avatar on the top right of the other forty-nine users' screens. A right-click at any moment would indicate what that person was doing, and an option would notify the authorities (either public or private) about suspicious activities.[71] This is one possible future to envision, where p2p principles are harnessed to augment security.[72] But there are serious costs, not just in terms of privacy, but also in terms of harm to the network. Realspace architects have found that it is often self-defeating to brightly illuminate areas to reduce crime—the upshot can be to scare users away from the street altogether and make the area look like "a prison yard."[73]

---

ana University banned all P2P applications" and that "[m]any other colleges have followed suit"), *available at* http://www.sandvine.com/news/article_detail.asp?ART_ID=21.

70 FATTAH, *supra* note 67, at 135-41. P2P may even offer a reliable strategy to blunt the force of denial of service attacks by dispersing the placement of content across the Net. *See* IRIS: INFRASTRUCTURE FOR RESILIENT INTERNET SYSTEMS, *at* http://iris.lcs.mit.edu (last visited Nov. 20, 2004).

71 As children taught about wolves and crying quickly learn, if a user falsely blew the whistle too many times, law enforcement would not take their warnings seriously. Conversely, users who give law enforcement helpful information would develop positive reputations around their pseudonyms.

72 As an alternative to gathering ISP customers, the system could randomly group users of a specific site together. When someone signs onto, say, Chase-Manhattan Bank, she could be bundled with fifteen other users, identified by avatar and pseudonym. A right-click would have the same function of revealing activities and enabling reporting to law enforcement.

73 Jackie Spinner, *The Jury's Out on Hotel's Lights; Dupont Circle's Bulbs Divide Community*, WASHINGTON POST, Feb. 23, 2001, at E01; *see also* MARK BRODUER, ARE TREES KILLING YOUR DOWNTOWN?: TOP TEN TIPS FOR DESIGNING A CONSUMER FRIENDLY DOWNTOWN, *at* http://www.dcn.davis.ca.us/go/wmaster/cda/newslet/nl0302/newslet.html#story4 (last visited Nov. 20, 2004) (discussing the "negative affect" on "strolling and shopping" when lighting is too bright); Katyal, *supra* note 4, at 1057 (discussing how particular forms of lighting can reduce natural surveillance).

The drive to illuminate cyberspace, and harness the surveillance powers of peers, thus has the potential to scare people away from the Net, instead of encouraging them to use it. As ISPs begin thinking about using such surveillance methods, their actions may generate negative externalities on the community in cyberspace more generally. As such, we should resist any government pressure to illuminate cyberspace because doing so can harm the network as a whole. And we should be developing security solutions that blunt the tendency of providers to over-illuminate their space in the name of reducing computer crime. In other words, the threats to anonymity and other (far more significant) forms of freedom on the Net do not simply originate from the state; preventing cybercrime through law and public architecture can forestall attempts to restrict these freedoms by private actors.

Illumination is one of many examples in which subtle cues from the environment can alter crime rates. In recent years, much of the realspace research about such cues has fallen under the rubric of "the broken windows theory" of crime control, which posits that visible disorders should be punished because they breed further crime. The insight of its two original authors, James Q. Wilson and George L. Kelling, was that these disorders are not always the most serious crimes like murder and rape, but instead could be as trivial as loitering and littering.[74] Wilson and Kelling thus inverted the standard thinking about enforcement and suggested that it was more effective to focus on low-level crime. As crimes become more common, the norms that constrain crime erode, and more crimes take place as a result of that erosion. But Wilson and Kelling, in their attempt to stimulate legal reform, wrongly downplayed the role of architecture in solving the problem that they brilliantly identified.[75]

Just as certain realspace architectural choices can facilitate certain forms of crime, computer programs can be written in ways that cue cybercrime as well. Consider Bearshare, a file-sharing program that operates on the Gnutella p2p network. Unlike many other file-sharing programs, Bearshare's "monitor" feature allows a user to see all the requests that are being

---

74 *See* James Q. Wilson & George L. Kelling, *Broken Windows*, ATLANTIC MONTHLY, Mar. 1982, at 29.

75 Wilson and Kelling claimed that high levels of crime were a response to a breakdown in social order, and that the solution to the breakdown was to reform police practices. Yet Wilson and Kelling's conclusions are somewhat suspect since they were derived from a study of the New Jersey Safe and Clean Neighborhoods Program, a program that not only changed law enforcement, but changed architecture as well. These architectural changes went unmentioned in their article, prompting cities like New York to follow the law-enforcement-centered approach to broken windows. *See* Katyal, *supra* note 4, at 1078-83 (describing how Wilson and Kelling ignored New Jersey program's design-based features and the role of architecture more generally).

made of the Gnutella network in real time.[76] Within twenty seconds, a user will glimpse dozens of requests for grotesque pornography, top-forty songs, and the like that flood the system. The user sees only the requests, with no user name or even IP address attached to them. Such visibility can induce crime—suggesting potential files available on the network—and can reduce the psychological barriers to downloading certain forms of content. By creating the perception that downloading such files is common, the architecture of the Bearshare program thus can generate additional crimes.

Computer programs must carefully control the cues that prompt crime, such as this Bearshare monitor feature. In realspace, environmental psychologists have shown that architects can manipulate subtle details to induce massive changes in behavior. The size and shape of tables will predict who talks to whom; the placement of lights in a lobby will make it easy to know where people will stand; the hardness of a chair will force people to get up quickly.[77] Digital architecture has similar properties.[78] Small changes to the way in which programs operate may have significant payoffs because digital architects can manipulate (indeed, already are manipulating) tastes in hidden ways. Greater private attention to the subtle aspects of design may thus prompt greater crime control and sidestep some need for public enforcement.

Reputational Screening. Because lighting up cyberspace poses numerous technical obstacles, as well as dangers to individual rights, it is worth thinking about less radical peer-based alternatives. Communities in realspace constantly deal with a related illumination problem – individuals have to transact with one another on specific matters without knowing the entire life history of one other. Joe sells widgets to Bob, and does not know much about Bob's previous dealings with other sellers or his loyalty in other spheres of life. It turns out, of course, that realspace communities have a good way of handling this – reputation. Joe learns about Bob's dealings through word of mouth: other sellers may talk to Joe about Bob, friends of Bob (and enemies) may reveal private information, and so on. Reputation becomes the glue by which contracts are struck and networks expanded.

---

[76] *See* BEARSHARE, BEARSHARE PRODUCT DOCUMENTATION, *at* http://www.bearshare.it/help/monitor.htm (last visited November 13, 2004) (describing the monitor feature).

[77] Katyal, *supra* note 4, at 1043-44, 1072-73. As Lawrence Speck, the Dean of the University of Texas School of Architecture puts it, architecture operates "much more [on the] subconscious than [the] conscious. Architecture is all about subliminal experience. . . . You listen to music, you look at a painting. But you live in architecture, and it affects you whether you're even conscious of it." Avrel Seale, *Architect Lawrence W. Speck and "The Vision Thing,"* TEXAS ALCALDE, July-Aug. 1999, *available at* http://txtell.lib.utexas.edu/stories/s0007-full.html.

[78] To take obvious examples: A link can be placed on the home page, in a prominent font and color, or placed in a space that requires users to scroll down.

Due to the darkness of cyberspace, pressure will mount to adopt reputational solutions that harness the power of the community, particularly as cybercrime increases. Already signs of this are beginning to emerge. A prospective buyer might "google" a company before buying its product, letting the power of the community inform its judgment. That buyer may instead go to a website such as bizrate.com or epinions.com that is devoted to consumer feedback about the company and its products. Such strategies permit some light to be shed on the past dealings of the company, thereby facilitating interactions between trustworthy sellers and buyers.

In its most sophisticated form, eBay has launched an extensive ability to rank reputations of both sellers and buyers. Each person who buys or sells a product is subject to a ranking by the other party to the transaction. High reputations function much as they do in realspace – consumers flock to stores that have them and are willing to pay premiums for their products. Economic studies reveal that such reputation ratings facilitate trust and transactions.[79] A decentralized reputational scheme like eBay's will permit enormous amounts of data to be brought out into the open, thereby illuminating some aspects of cyberspace that would previously have been left dark.

The eBay model of cybersecurity at this juncture seems inevitable. If enough saboteurs to networks and commercial activity proliferate, some sort of reputation-based screening is going to become essential. Whether that screening is tied to one's IP address, email account, biometric data, or some other mechanism, the point is that individuals will have to invest in their reputations to distinguish themselves from the dangerous and untrustworthy. The trick will be to come up with ways for reputations to be exchanged across different portals. When Amazon.com tried to let sellers place their eBay reputational rankings on the Amazon auction website, eBay objected, claiming the information was proprietary.[80] In the commercial setting, side payments might prevent the problem from arising very often, but as reputational ranking becomes standard in noncommercial transactions, a need will arise to break down the barriers to information flow for stronger cybersecurity.

Of course, the very fact that Amazon wanted to use eBay's reputation systems points to a public goods problem. If eBay had to turn over that information to other vendors and purchasers, then it would never deign to

---

[79] *See* Sulin Ba & Paul A. Pavlou, *Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior*, 26 MIS QUARTERLY 243 (2002); GARY BOLTON ET AL., TRUST AMONG INTERNET TRADERS: A BEHAVIORAL ECONOMICS APPROACH 19, *available at* http://ockenfels.uni-koeln.de/download/papers/trust_03022004.pdf (Feb. 2004) ("sellers' intrinsic motivations to be trustworthy are not sufficient to sustain trade when not complemented by a feedback system. Translated to Internet market platforms, it seems likely that eBay or Amazon's market for used books would quickly collapse without a reputation system.").

[80] Ba & Pavlou, *supra* note 79, at 263.

collect the information in the first place. eBay's data collection would be costly and its benefits would not redound to the corporation alone. The reputational problem suggests the need for an independent entity, perhaps operated by the government, that collects all of this information in a centralized place and makes it available to the panoply of consumers and sellers. That is the type of community self-help model envisioned at the outset of this Section: a realspace prevention model whereby government sets up a framework and then the community provides the relevant information. A government-centralized and subsidized resource center would not only expand the reach of the reputational rankings, it could help augment trust in them. At the same time, it would minimize the distributional concerns that inhere in a completely private self-help system.

3. The Problems with Offensive Self-Help: The Counterstrike Example

The fact that community-based solutions have promise does not mean that all of them are good ideas. Consider one exemplar of some of the problems with self-help strategies: the so-called "counterstrike" option. The impetus for counterstrike is the realization that defensive techniques are too costly or will not work.[81] As Ross Anderson describes the problems with defense, "Defending a modern information system could also be likened to defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere."[82] That difficulty has led an increasing number of security managers to advocate attacking offending computers. By doing this, the argument goes, victims can avoid the problem of relying on the police.[83] If companies would disable machines that promulgate worms before they take up bandwidth, the victims would save money and resources.[84] Offensive measures would have other advantages, too. They sidestep difficulties such as lengthy prosecutions, thorny jurisdictional matters, technologically unsophisticated juries, and slow courts.

---

81 *See* Paul A. Strassmann, *New Weapons of Information Warfare,* COMPUTERWORLD, Dec. 1, 2003, at 41, *available at* http://www.strassmann.com/pubs/cw/new-weapons.shtml; TIMOTHY M. MULLEN, DEFENDING YOUR RIGHT TO DEFEND: CONSIDERATIONS OF AN AUTOMATED STRIKE-BACK TECHNOLOGY, *at* http://www.hammerofgod.com/strikeback.txt para. 4 (Oct. 28, 2002) (defensive techniques cost a company "money in bandwidth, router, and server utilization.").

82 Ross Anderson, *Why Information Security is Hard- An Economic Perspective,* 17TH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE 5 (2001), *available at* http://www.acsac.org/2001/papers/110.pdf.

83 *See* Winn Schwartau, *Cyber-Vigilantes Hunt Down Hackers* (Jan. 12, 1999), *at* http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/.

84 *See* MULLEN, *supra* note 81.

And counterstriking against those who attack computer systems can provide satisfying and instant revenge that other methods cannot.[85]

I reject the notion that counterstrike proposals are by their nature "unjust." For example, Bruce Schneier, with whom I agree on much, argues that the target of a counterstrike has been found guilty without receiving a fair trial.[86] But that point can be said about any self-defense regime, and the criminal law permits self-defense in a variety of situations. (The common law also permits self-help against nuisance, which is another promising analogy.[87]) At common law, there are three major requirements that a person must satisfy to justifying using force to protect his property in self-defense. First, the actor must either request that the criminal stop his conduct, or reasonably believe that such a request would be futile or counterproductive. Second, the actor must reasonably believe that force is necessary to prevent the harm.[88] And third, he must only use a reasonable amount of force.[89] It may be difficult for counterstrikes to satisfy these three requirements, particularly the latter two, but if they do, it is not "unjust" for someone to exercise self-defense.

However, counterstrike systems have two other problems. First, a counterstrike may hit the wrong person or target. While an exercise of self-defense in realspace might wound a bystander, in cyberspace the circle of potential bystanders can be far greater. Second, counterstrikes may cue crime instead of diminish it. Both of these points originate out of work done in criminology about the relationship between crime and community. They suggest that a shift towards counterstrikes might fragment networks even further and fail to protect them. And looming here, as always, is the distributional concern, that a counterstrike regime will not protect those who need it the most.

---

85 *See* Curtis E. A. Karnow, *Launch on Warning: Aggressive Defense of Computer Systems*, 8 No. 1 CYBERSPACE LAWYER 4 (Mar. 2003), *available at* http://islandia.law.yale.edu/isp/digital%20cops/papers/karnow_newcops.pdf.

86 *See* Bruce Schneier, *Counterattack*, CRYPTO-GRAM NEWSLETTER (Dec. 15, 2002), *at* http://www.schneier.com/crypto-gram-0212.html.

87 *See* Karnow, *supra* note 85, at 9; Douglas Ivor et. al., *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society* (pt. 1), 37 VAND. L. REV. 845, 868 (1984) ("The privilege to summarily abate a nuisance is a self-help remedy arising from property interests that has existed at least since the earliest reported cases.").

In a lower court appeal of *Intel v. Hamidi*, the Electronic Frontier Foundation urged the court to move to nuisance rather than a "trespass to chattels" doctrine in evaluating whether a former employee's mass e-mailings to Intel workers were a tort. *See* Electronic Frontier Foundation Amicus Brief, Intel Corp. v. Hamidi, 114 Cal Rptr. 2d 244 (Cal. Ct. App. 2000) (No. C033076), *available at* http://www.eff.org/Spam_cybersquatting_abuse/Spam/Intel_v_Hamidi/20000118_eff_amicus.html.

88 This requires that the actor subjectively and reasonably believe that he will imminent lose his property unless he uses force. *See* Jurco v. State, 825 P.2d 909 (Alaska Ct. App. 1992); Doby v. United States, 550 A.2d 919 (D.C. 1988).

89 *See* RESTATEMENT (SECOND) OF TORTS § 77.

First, a large risk looms that overzealous defenders may strike the wrong party. With the notable exception of the Fourth Amendment, the same problems that make it hard for law enforcement to track cyber-offenders also make tracking hard for counterstrikers. "Without effective intrusion source tracing, no effective countermeasures such as containment, redirection, or back-hacking can be implemented."[90] It is possible that the private sector may be able to respond to an attack in realtime, whereas law enforcement may not always have that capability. But nevertheless, tracing is tough, even in realtime, and the risk of identifying the wrong party is high. And even with excellent tracing, sometimes multiple people will be employing the same computer. For example, a young hacker may use his grandmother's computer to commit an attack and a counterattack against that computer may destroy valuable data and harm the grandmother.[91]

The counterstrike discussion thus far has involved a surgical attack only against one other computer. But some counterstrike proposals go much further, such as those in favor of "white hat" viruses designed to inoculate computers from the effects of another virus. In these cases, viruses, even "beneficial" ones, may have unpredictable consequences for the stability of platforms and applications. Anyone who doubts this should try running the Windows Service Pack 2 update.

A few additional drawbacks are raised by misidentification, apart from the simple injustice of it. One is that a counterstrike world is one in which, paradoxically, everyone's barriers need to be even higher. Precisely because counterstrikes will land on innocent computers, those who wish to protect the integrity and privacy of their data will need to build defenses. But if the entire premise of counterstrike is that these defenses are too expensive or too difficult to run against an enemy that might be anywhere, then the entire project becomes self-defeating. Indeed, it may lead to perverse network effects as people build stronger firewalls because they cannot trust law enforcement and similarly cannot trust the counterstrikers.

Misidentification also has distributional drawbacks. Even if current technology can trace some cybercriminals, allowing offensive self-help will invariably mean that those with less technical skill will have to compete with advanced cybercriminals, often with disastrous results.[92] For example, an advanced hacker could use his knowledge about hack-back to route an attack through a hospital computer or other critical infrastructure, leading to

---

[90] *See* Vikas Jayawal & William Yurcik & David Doss, *Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?* (2000), at 2, *at* http://dump.cryptobeacon.net/papers/ISTAS02hackback.PDF.

[91] *Id.* at 2. In 1997, a large accounting firm shut down several routers of a major ISP because it believed it was about to be the victim of a denial of service attack. This overreaction shut down Internet access for many Sprint users. *See* Schwartau, *supra* note 83.

[92] *See* Susan W. Brenner, *Distributed Security: Moving Away From a Reactive Model of Law Enforcement*, *at* http://islandia.law.yale.edu/isp/digital%20cops/papers/brenner_newcops.pdf

a harmful counterattack against an innocent party.[93] And it is far more likely that those who will be unable to self-protect against misidentified counterstrikes will be the poorer segment of users, leading to the same form of regressiveness as the automobile example in realspace discussed in Part I of this Essay.

A second major problem with counterstrikes is that they can create the perception of insecurity. Counterstrikes resemble the clumsy patches to the system we saw in realspace, and the upshot may be to diminish people's confidence in the security of the network. Counterstrikers do not have the same public-minded spirit of law enforcement, instead they are driven by self-interest. The entire premise of counterstrike is that the system cannot handle the problem. As such, their use can act like a broken window, cuing a belief that the Net is insecure.

Additionally, there are good reasons to think that counterstrikes might provoke or increase crime. Hackers who become targets of counterstrikes may respond by escalating their attacks, leading to a cycle of Internet violence.[94] As one ex-hacker observed, "If my machine crashed and I've been hacking... I would not give up then. If hackers gave up so easily there would not be any hackers. It's the challenge."[95] After all, many hackers commit crimes to show off their technical prowess. Counterattacking cyber criminals would not deter these hackers, and may prompt more cybercrime.[96] A universe of computer users that kept shooting back at one another would create a huge dead-weight loss, and may make the Internet a more dangerous and less pleasant place for all.

Consider two popular examples of counterstrike that are ridden with these problems. During the 2002 Blackhat briefing in Las Vegas, Timothy Mullen proposed that computer owners should be able to use an automated program to strike back at Nimda-infected machines. This program would work by exploiting the same vulnerability that allowed the worm to promulgate and would prevent that worm from starting up on the infected com-

---

93 *Id.* at 4-5; *see also* Karnow, *supra* note 85, at 5 ("Not all attacks will so plainly reveal a path back to their source as did CRII; tracing an attack to an intermediate attacking machine, not to speak of the computer owned by the originator in a DDOS attack, may be impossible. And intermediate machines, or zombies in a DDOS attack, may be operated by hospitals, governmental units, and telecommunications entities such as Internet service providers that provide connectivity to millions of people: counterstrikes which are not very, very precisely targeted to the worm or virus could easily create a remedy worse than the disease.")

94 *See* Landergren *supra* note 60.

95 *See id.*

96 *See* Chris Loomis *Appropriate Response: More Questions Than Answers* (November 28, 2001), *at* http://www.securityfocus.com/infocus/1516 (reporting the view that "There isn't any evidence that digilantism has any appreciable deterrent effect. Take out an attacker's zombies and he'll get more. Take out an attacker and he'll be back - and more determined.").

puter.[97] Mullen characterized his plan as "purely defensive" because the technology only neutralized the attacking process and did not attempt to harm the infected machine.[98] Mullen claimed that this technique would merely stop the worm from propagating and would not remove the worm from the target computer or even patch the original vector.[99] On the other hand, this technology involved inserting a command into the target computer's boot sequence to prevent the worm from starting up.[100] It introduced this command into *any* computer that is infected with the worm, regardless of whether its owner played a knowing role in creating or promulgating the worm.

One can see the self-help proponents justifying this type of solution. After all, a security officer using this method would not need to rely on police to protect his system, avoiding jurisdictional and inefficiency pitfalls. It would give some measure of relief to scrupulous computer owners who are victims of attacks by hackers who weave their assault through third-party computers that are not protected against being turned into a launching pad for attacks.[101] And it would promote herd immunity—the concept that even if my child is not vaccinated, the vaccinations of others will prevent my child from being infected. Such a counterstrike might also supplant traditionally defensive measures that are less efficient because they involve significant resources and bandwidth.[102]

But of course this proposal means that counterstrikes would be launched against any computer harboring the worm, not just active wrongdoers. That lack of restraint poses numerous problems, most particularly if the counterstrike interferes with the functions of an "innocent" computer. And even if the computer itself might not be harmed by the counterstrike, the unleashing of such a program could itself disrupt network connections. Here we should remember the lesson of the CodeGreen patch, which was developed as a countermeasure to the Code Red worm. CodeGreen was a well-intended worm patch, but like the worms it meant to attack, it ended up wasting bandwidth and clogging numerous systems.[103] Mullen's particular program might have been carefully designed, but as *Markus DeShon*

---

97 *See* Mullen, *supra* note 81 (explaining his proposed technology); Timothy M. Mullen, *The Right to Defend* (July 29, 2002) (short column defending the right to strike back using the neutralizing method), *at* http://www.securityfocus.com/columnists/98.

98 *See* Mullen, *supra* note 81.

99 *See id.*

100 Markus DeShon, *Hackback or the High Road? The Question Goes Beyond Nimda* (September, 20 2002) (criticizing Mullen's proposal as setting a dangerous precedent) *at* http://www.securityfocus.com/guest/16531.

101 *See* Mullen, *supra* note 81.

102 *Id.*

103 *See* DeShon, *supra* note 100.

puts it, "the precedent is there – and subsequent counterattacks may not be as robust as Mullen's."[104]

Even if counterstrikes could be surgically crafted so as to have no perverse effects, they may still diminish faith in the Net's security. As one observer put it, "It's like having a seasoned criminal break into your house and then, if he succeeds, install an alarm system."[105] The first thing that someone would do in that realspace setting is get a better lock. Cyberspace is no different. Counterstrikes have the potential to fragment people's confidence in the Net. That said, individual counterstrikes are far worse than community ones. If a large number of users write a patch (or bless it), it would lower the risks of misidentification and may be more likely to generate confidence in the network.

Consider another proposal that has received much attention of late. Several members of Congress have proposed ambitious plans that would allow copyright owners to hack back against those who violate their copyright. A bill introduced by California Democrat Howard Berman in 2002 legally immunizes copyright owners who blocked, diverted or otherwise impaired unauthorized distribution of their work on peer-to-peer networks.[106] The bill does not specify what counterattack methods the copyright owner may use, but does say that they could not involve file deletion.[107] Senator Orrin Hatch has gone one step further and implied that copyright owners might be allowed to destroy violators' computers without fear of legal liability.[108]

One justification for these proposals is that copyright owners have been unable to stop the illegal trading of copyrighted material on peer-to-peer networks. The Recording Industry Association of America has brought numerous lawsuits against users and has begun authorizing use of pay-per-song services like iTunes.[109] Yet, illegal file swapping continues at a robust pace, with many users moving from larger networks like Kazaa to smaller ones like iMesh, BitTorrent and eMule.[110] Engaging in widespread lawsuits is far more expensive that using offensive tactics against file traders.

---

104 *Id.*

105 Paul Roberts, *New Variant of Blaster Worm "Fixes" Infected Systems* (August 19, 2003), *at* http://www.computerweekly.com/Article124251.htm.

106 H.R..5211, 107th Cong. (2002), *available at* http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.5211.

107 *Id.*

108 *See* Declan McCullagh, *Senator OK with Zapping Pirates' PCs* (June 18, 2003), *at* http://news.com.com/2100-1028_3-1018845.html.

109 The industry has brought suit against thousands of music swappers. Reuters, *RIAA Sues 493 More Music Swappers* (May 24, 2004), *at* http://zdnet.com.com/2100-1105_2-5219114.html.

110 *See* Dawn Kawamoto, *Downloads Rise as File Traders Seek New Venues* (April 26, 2004), *at* http://zdnet.com.com/2100-1104_2-5199901.html.

Here again, the same problems with counterstrike emerge. The risk of misidentification looms. And there is, after all, a track record: the RIAA has made mistakes before, like when it sent a cease-and-desist letter to an ISP, which included a list of files supposedly copyrighted by George Harrison. Unfortunately, some of the files contained in this letter included "Portrait of mrs harrison williams 1943.jpg."[111] Moreover, the RIAA has had to apologize for sending a threatening letter to Penn State University that falsely alleged Internet copyright violations.[112] The error occurred because the RIAA mistakenly identified a speech on radio-selected quasars by Professor Peter Usher as an illegally downloaded song by performing artist known as "Usher."[113] Such examples illustrate the dangers of allowing legalized counterstrikes by private entities. In these cases, the letters did little damage and the problems were cured with judicial oversight and an apology. Under the Berman and Hatch proposals, however, these same mistakes could have led to disabling Penn State University's FTP site or even destroying its computers. Such a possibility is dangerous for individual users, who would have fear that unfortunate names of files (like "mrs. harrison williams") could cause them to become targets of mistaken but legal counterattacks.

If counterstrikes against music began, the result could be to harm digital music and stores like iTunes instead of helping them grow. Individual computer users would fear misidentification at every turn, leading them to restrict network access to their computers and data by unplugging their hard drives or even their internet connections. It would begin to resemble the balkanized networks discussed in Part I. A world in which people are scared to get online for fear that some infringing material might be located on their computer is not one conducive to growth of the network.

III. CONCLUSION

The community is an institution of balance and ballast. Conventional approaches to crime control made the mistake of emphasizing public enforcement too much, neglecting the fact that crime can often be prevented more cheaply through the actions of private individuals. But the modern corrective to the conventional story has gone too far in the other direction, making it appear as if private self-help can accomplish everything law enforcement can while providing efficiency gains. In truth, private self-help

---

111 Peer-to-Peer File Sharing Privacy and Security: Hearing Before House Committee on Government Reform, 108th Cong., n.16 (2003) (Testimony of Alan Davidson, Associate Director, Center for Democracy and Technology), *available at* http://www.cdt.org/testimony/030515davidson.pdf.

112 Declan McCullagh , *RIAA Apologizes For Threatening Letter* (May 12, 2003), *at* http://news.com.com/2100-1025_3-1001095.html.

113 *See id.*

runs the risk of atomizing societies and increasing crime rates, and poses severe distributional concerns as well.

The community self-help approach, by contrast, mitigates some of the drawbacks of each system by recognizing that the private and public sectors must temper a robust dialogue with an engagement in the promise of cooperation. By harnessing the strength of private individuals who are often best situated to control crime, community strategies can be more efficient than conventional policing ones. But by anchoring self-help to community institutions, the tendency of groups to act in extremist, and perhaps retributive, ways is avoided and some of the dangers of societal fragmentation are reduced.

Community self-help strategies in realspace have shown that they have the capacity to reduce crime rates. When neighborhoods share information about criminals with police, when law enforcement partners with citizens to devise joint approaches to controlling crime and launches "neighborhood watch" programs, and when local officials share information with residents about architectural approaches to minimizing crime, criminal acts can decline and the community can be strengthened simultaneously.

The challenge today is to understand whether similar strategies are available in cyberspace. With a fragmented community not tethered to realspace, the barriers to community self-help are many. But because the ease of participation is so much greater than it is in realspace, promise abounds. It is time for the public and private sectors to begin exploring how to harvest that promise.

SELF-HELP AND THE NATURE OF PROPERTY

Henry E. Smith[*]

I. INTRODUCTION

Self-help and the law's response to it lie at the center of a system of property rights. This has become all the more apparent as questions of property – and whether to employ property law at all – have arisen in the digital world. In this Article, I argue that self-help comes in different varieties corresponding to different strategies for delineating entitlements. Like property entitlements more generally, the law does not regulate self-help in as detailed a fashion as it could if delineation were costless. Both property entitlements and self-help show far less symmetry and a far lesser degree of tailoring than we would expect in a world in which we did not face delineation costs of devising, describing, communicating, and enforcing the content of rights and privileges to use resources.

Part II of this Article sets the stage for an analysis of self-help by showing how the law-and-economics treatment of entitlements leads one to expect greater symmetry in entitlements than is to be found in the law. In the commentary, rights to be free from pollution are paired conceptually with so-called rights to pollute, but the law does not provide for free standing rights – as opposed to occasional privileges – to pollute. Part III shows how these apparent anomalies receive an explanation on a theory of entitlement delineation that accounts broadly for costs as well as benefits. Roughly speaking, the law faces a choice among strategies for delineating entitlements, and in the choice among these strategies, the benefits of multiple uses of resources must be traded off against the costs of delineation and enforcement. On the one hand, one can delineate entitlements using very rough signals that protect uses indirectly but do not refer to uses specifically, which I call an exclusion strategy. The right to exclude from Blackacre is the prototypical example. Or one can tailor entitlements to important uses in order to capture the benefits of multiple uses, but at a higher delineation cost. This I call a governance strategy, and various off-the-rack nuisance rules and land use regulations as well as privately negotiated easements and covenants would be examples. Normatively, the law should provide off-the-rack governance schemes only when the stakes are high and more cost-effective tailored governance rules cannot be expected to emerge from private parties themselves. More positively, much of the

* Professor of Law, Yale Law School. E-mail: henry.smith@yale.edu. For helpful comments I would like to thank audiences at Dartmouth and George Mason University. All errors are mine.

costs of delineation identified here are internalized to those who are called upon to devise and enforce property entitlements. Part IV demonstrates that the law's approach to self-help is intertwined with and reflects the same cost-benefit considerations as the general system of entitlements. Part V turns to self-help in the digital arena and shows how controversies over trespass to websites, digital rights management, and copyright fair use reflect the place of self-help within a system of entitlement determination that mixes elements of exclusion and governance. Part VI concludes.

II. THE MISUSES OF SYMMETRY IN THE LAW AND ECONOMICS OF PROPERTY RIGHTS

Like many a would-be science, law and economics has always sought out symmetry as a source of explanation. In law and economics, many of these symmetries are supposed to characterize the shape of entitlements. To take the classic illustrative example, the "entitlement" to pollute can be located in the polluter or the victim. The symmetry of entitlement placement reflects what legal economists, following Coase, see as the reciprocal – symmetric – nature of causation.[1] Indeed the polluter or the victim can equally easily be regarded as the cause of the conflict. In the area of self-help, this would lead us to say that either the one engaging in self-help or the one acted upon can be regarded as the cause of the interaction. Taken to the extreme, someone acting in self-defense would be the cause of conflict just as much as the original threatener. But this is an unintuitive and unattractive feature of the reciprocal view of causation: in an everyday sense we do not say that the owners of noses cause punches as much as the owners of the fists that impact them. The policies for placing liability suggested in the law and economics literature, such as lowering bargaining costs or choosing cheapest cost avoiders for liability, do not fully explain our assignment of liability to those who cross boundaries. Or at least, so I will argue.

Like many of the symmetries in physics that hold only at high energies, many of the symmetries that law and economics is built upon only hold in a world of vanishingly low transaction costs. Once positive transaction costs come into the picture, there is a ready explanation for why entitlements – and those entitlements typically labeled "property" in particular – do not show the degree of symmetry expected of them. While on one level scholars realize that the world of zero transaction costs is a theoretical construct meant to illustrate the importance of transaction costs in the real world, this lesson has not been carried over sufficiently into the question of the shape and delineation of entitlements, the core questions in the theory of

[1] Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 2, 8-15, 35 (1960).

property.[2] I will argue that once certain types of (positive) transaction costs are taken into account, we can explain why property is so radically non-symmetric in that there are invaders and victims, and in that boundary crossings are crucial to liability.

Property law has been surprisingly neglected in law and economics. In one sense, of course, this is untrue. Law and economics is all about "property rights" and "entitlements." But these have little to do with the traditional subject matter of property, and if anything the thrust of law-and-economics analysis calls into question some of the core notions built into actual property law – rights to exclude and invasions based on who did what where.[3]

One of Coase's contributions along these lines was to challenge the notion that in resource conflicts we can identify who caused the harm. Where cattle are trampling corn, we can say that cattle and corn are competing for the same space and that the corn is in the way of the cattle as much as (conventionally we tend to say) the cattle are damaging the corn. If a farmer has a right to be free from trampling damage, then the farmer is causing the rancher harm just as much as if the rancher's cattle could destroy the farmer's crop without liability. Or to take another famous example, if a confectioner builds a grinding machine on a party wall on the other side of which a medical doctor has his examining room, we might tend to say that the confectioner is harming the doctor because he is causing the noise.[4] But the doctor's need for quiet causes the confectioner harm in equal measure, according to Coase.[5] Where it is not wealth-maximizing for cattle and crops or medical exams and candy-making to occur simultaneously, the source of the conflict is equally in each of the parties.

Coase pointed out that in a world of zero transaction costs the parties would bargain to the wealth-maximizing solution to the resource conflict regardless of who had the initial entitlement.[6] The potential payment to

---

[2] Coase was very clear that in the analysis of actual situations positive transaction costs are key. *Id.* at 15-19; *see also* RONALD H. COASE, THE FIRM, THE MARKET, AND THE LAW 15 (1988). I will be arguing that by not taking the transaction cost implications of his realist bundle-of-rights assumptions about property seriously enough, Coase did not apply the lessons of positive transaction costs broadly enough.

[3] *See, e.g.*, Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357 (2001); Henry E. Smith, *Exclusion and Property Rules in the Law of Nuisance*, 90 VA. L. REV. 965 (2004).

[4] Coase, *supra* note 1, at 8-10 (discussing *Sturges v. Bridgman*, 11 Ch. D. 852 (1879), involving a confectioner and a doctor).

[5] *Id.* at 9-10.

[6] *Id.* at 2-15. How this proposition needs to be qualified has been controversial. On wealth effects, see, for example, Harold Demsetz, *When Does the Rule of Liability Matter?*, 1 J. LEGAL STUD. 13 (1972); Stewart Schwab, *Coase Defends Coase: Why Lawyers Listen and Economists Do Not*, 87 MICH. L. REV. 1171, 1178-84 (1989) (book review of RONALD H. COASE, THE FIRM THE MARKET AND THE LAW); but compare COASE, *supra* note 2, at 170-74. On strategic behavior, see, for example,

cease activity is as much a cost as any other, and in the zero-transaction-cost world there is no impediment for these offers to be made and accepted. But Coase went further. In a world of positive transaction costs, the goal should be to take into account the effect of decisions on the value of production and, in that sense, to mimic the zero-transaction-cost world.[7] Because transaction costs are a barrier to the making and acceptance of side payments, the initial location of the entitlement can matter. But when he moves to the actual positive-transaction-cost world, Coase does not give up entirely on the type of symmetry he identified in the zero-transaction-cost world. Because either of the parties to a resource conflict can equally be said to be causing the conflict, there is no reason to favor the one or the other with the initial entitlement – other than policy considerations like maximizing the value of production. The question becomes whether cattle or crops are more suited to a given location – or candy-making or medical exams, or whatever. There is no *a priori* reason to think that crops or medical exams should be regarded as victims and ranchers and confectioners as injurers.

This type of symmetry argument is deeply engrained in law-and-economics thinking, but let me raise an initial question about it. Notice that there is some asymmetry built into these interactions, an asymmetry reflected in everyday notions of causation and harm. If the activity of the farmer or the doctor is going to survive, either liability must be placed on the other party or the person in the position of the farmer or doctor must take some form of self-help. This self-help can be passive as in building a fence or in soundproofing a party wall, or more active, as in shooting the cattle or smashing the noisy pestle. By contrast, the rancher and the confectioner tend to do better in the state of nature. Putting aside the possibility of "active" self-help on the part of the other party, a situation of no liability would suit the rancher or the confectioner just fine. Cattle will win the competition with crops, and noisy activities like candy-making will win out over medical exams. The entitlement needed to protect these more robust activities is more minimal than the one needed to protect the more vulnerable ones. Thus, there is already an asymmetry in terms of the entitlement needed to protect the conflicting activities in order for them to prevail.

Furthermore, another related source of asymmetry reflected in everyday notions of causation centers on location. When activity moves physical objects across a boundary or leads to collisions we tend to say that the activity caused the harm that results. Thus, if someone showers pellets on someone else's land or sends in odors, we tend to say that person is a tres-

---

Robert Cooter, *The Cost of Coase*, 11 J. LEGAL STUD. 1 (1982), for a comparison of the Coase theorem and the "Hobbes Theorem."

[7] Coase, *supra* note 1, at 19.

passer or the creator of a nuisance rather than the other way around.[8] Even more obviously, when A punches B in the nose, A is usually regarded as causing the harm, not B (or B's nose). By contrast, in the zero-transaction-cost world, Coase is right that location is irrelevant. We could assign liability for pellets, odors, and punches to A or B – or to any C – for that matter.[9] Bargaining would take care of the rest.

But in the world of positive transaction costs, I argue, boundaries and protected objects are a more economical way to delineate entitlements than specifying all the activities holding between all pairs of people in society and assigning entitlements on that highly atomized basis. Positive transaction costs systematically favor one set of entitlements over another, leading to the asymmetry we observe in real world entitlements. Once again, law and economics, following Coase, simply assumes that more of the symmetry rightly identified in the zero-transaction-cost world carries over into our own world of positive transaction costs.

This overextension of symmetry to situations of positive transaction costs is also characteristic of Guido Calabresi and A. Douglas Melamed's famous "Cathedral" framework of property rules and liability rules.[10] Following Coase, Calabresi and Melamed (C&M) noted that an entitlement could be located in either the "injurer" or the "victim." To use their primary example of air pollution, the entitlement to be free from pollution could be given to the Resident, or the entitlement to pollute could be given to the Polluter.[11] Just as the costly interaction can be characterized as involving reciprocal causation, the entitlement can be given to either party: the possibilities for assigning entitlements are symmetrical as well. C&M then noted that two methods of protection could be afforded this entitlement.[12] In one method, the entitlement could be protected with robust remedies such as injunctions and punitive damages so that a would-be violator must negotiate a consensual transfer from the present holder. C&M called this a "property rule." Or, on another method, the would-be taker could be permitted to violate the entitlement as long as it pays compensatory damages, in what C&M called a "liability rule." Having identified two cross-cutting distinctions they argued that there should be four types of rules.[13] In Rule 1, the resident is protected from pollution through a prop-

---

[8] On the distinction between trespass and nuisance, see, for example, Thomas W. Merrill, *Trespass, Nuisance, and the Costs of Determining Property Rights*, 14 J. LEGAL STUD. 13 (1985); Smith, *supra* note 3, at 992-96.

[9] For an explicit recognition that liability could be assigned to an apparently unrelated party and an argument that this would make sense if that person were the cheapest cost avoider, see GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 68-69, 136 (1970).

[10] Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

[11] *Id.* at 1090.

[12] *Id.* at 1092.

[13] *Id.* at 1115-16.

erty rule; the resident can get an injunction to force the factory to stop polluting. In Rule 2, the resident still has the entitlement, but is only protected by a liability rule. The resident can sue the polluter, and the polluter will be allowed to continue to pollute but will have to pay compensatory damages to the resident. In some sense, the entitlement in the Rule 2 scenario is split in this case between the factory owner and the resident.

C&M then claim that by symmetry, the "entitlement" to pollute can be in the factory and protected by a property rule, which is Rule 3. As we will see, the details of this scenario are often left unclear, but at the least the resident cannot force the factory to stop polluting and the factory will enjoy the ability to pollute without having to pay anything to the resident. In C&M's words:

> Third, Taney [the polluter] may pollute at will and can only be stopped by Marshall [the resident] if Marshall pays him off (Taney's pollution is not held to be a nuisance to Marshall). . . . Rule three (no nuisance) is instead an entitlement to Taney protected by a property rule, for only by buying Taney out at Taney's price can Marshall end the pollution.[14]

This formulation betrays some uneasiness about the content of the supposed property rule protection for the polluter. I will argue that the law is in fact radically asymmetric in C&M's Rule 1 and Rule 3 scenarios, which supposedly give property rule protection for "the" entitlement in the resident and the polluter, respectively.[15] This leaves one more cell, and C&M deduced the possibility of a new Rule 4, under which the factory would have the entitlement but only protected by damages.[16] In other words, the resident could get an injunction to abate or shut down the pollution but would have to pay the factory's costs of doing so. Dramatically, at around the same time, the decision in the coming-to-the-nuisance case of *Spur Industries, Inc. v. Del E. Webb Development Co.*[17] seemed to adopt something like Rule 4, although Rule 4 has never been used in a nuisance case since.[18]

The problem in this elegant picture actually begins when C&M look for a symmetric entitlement in the polluter as in the victim. What does it mean for the polluter to have "the" entitlement? When the resident has the entitlement, the victim is vindicating its interest in the use and enjoyment of

---

14 *Id.* at 1116.

15 *See* Henry E. Smith, *Property and Property Rules*, 79 N.Y.U. L. REV. 1719 (2004); *see also* Jeanne L. Schroeder, *Three's a Crowd: A Feminist Critique of Calabresi and Melamed's* One View of the Cathedral, 84 CORNELL L. REV. 394, 412-17 (1999) (providing feminist critique of view that liability rules and property rules are alternate methods of protecting same entitlement).

16 Calabresi & Melamed, *supra* note 10, at 1115-16.

17 Spur Indus. Inc. v. Del E. Webb Dev. Co., 494 P.2d 700, 708 (Ariz. 1972) (en banc).

18 For a discussion of the popularity of Rule 4 in commentary on nuisance law and an argument against use of Rule 4, see Smith, *supra* note 3, at 1107-21.

its property as defined by the boundaries around the resident's parcel.[19] What about the polluter? The usual assumption – to the extent it is made clear – is that if the polluter has the entitlement, a suit by the resident will be dismissed; no nuisance will be found, as C&M put it.[20] But this is *not* symmetry in any meaningful sense. True symmetry would require that the polluter have not merely a privilege to pollute – "Taney may pollute at will" – but a *right* to do so, backed up by the possibility of an injunction. In the Hohfeldian scheme a right (or claim) is an entitlement that corresponds to a duty in another: if the resident has a right to be free of pollution, there is a corresponding duty in the polluter not to pollute.[21] Flipping things around, if the polluter has a similar entitlement, a right to pollute, then the resident has a *duty* to accept pollution and possibly a duty not to interfere with the passage of pollution from the factory onto her land. The polluter would be entitled to an injunction if the resident built fans or walls that impeded the flow of the air pollution onto the resident's land and away from the polluter. Such an entitlement does exist: it is called an easement. Unlike the resident's entitlement in the Rule 1 and Rule 2 scenarios, though, easements are *not* part of the default package of rights in land but only arise as special rights in the lands of another (along with real covenants).[22] These special rights are usually separately bargained for between the neighboring landowners.[23] The closest that the default package of rights comes to containing an "entitlement" to pollute is in the *privilege* to pollute that a landowner might have as long as neighboring landowners have no entitlement to be free of pollution.

The difference between an off-the-rack package and these special rights can be illustrated by considering adverse possession. Adversely possessing Blackacre will give the default package of rights in the fee simple, including the right to be free of trespasses and nuisances (Rule 1 and, sometimes Rule 2 protection). The adverse possessor may also acquire a *privilege* to pollute but will not have a right to pollute unless a special easement to commit what would be an actionable nuisance has been acquired through prescription, the analogue of adverse possession for use-rights.[24] In a zero-

---

19 For more detail on how the boundary is defined see *infra* note 26 and accompanying text.

20 For an unusually careful statement of Rule 3, see KENNETH S. ABRAHAM, THE FORMS AND FUNCTIONS OF TORT LAW 176-77 (2d ed. 2002).

21 WESLEY NEWCOMB HOHFELD, FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING AND OTHER LEGAL ESSAYS 23-64 (Walter Wheeler Cook, ed., Yale Univ. Press 1923), reprinting Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16 (1913).

22 *See* Smith, *supra* note 3, at 1001-02, 1017.

23 Easements and closely related covenants are sometimes placed in all the deeds in a development by developers. Again, this creates special rights through contract, not as an off-the-rack default set of legal entitlements.

24 Note that in some of the nuisance cases considered by Coase, including the famous case of *Sturges v. Bridgman*, 11 Ch. D. 852 (1879), the question was framed in terms of whether a prescriptive

transaction-cost world, this distinction between what rights are to be found in the default packages of rights and which are special or stand-alone rights would, of course, be irrelevant. But in our world, such considerations are of the greatest importance.

If we ignore easements for the moment and focus on these default, off-the-rack packages, a right to pollute is decidedly *not* the type of "entitlement" that the law grants polluters in the "Rule 3" situation. Rather, as the writers in the liability rule literature seem usually to assume – when they are clear on this point at all – in Rule 3, the factory owner has a *privilege* to pollute, not a right. In a Hohfeldian privilege to do X, the holder has freedom to do X and no one else has a right to invoke the law to stop it.[25] That is, if A has a privilege to do X vis-à-vis another actor B, this means that B has no right (or in Hohfeld's neologism a "no-right") to invoke the law to stop A from doing X. Just as a duty is the correlative of a right, a no-right is the correlative of a privilege.

The possibility of the entitlement being in the resident or the polluter is not symmetric. The resident might have the entitlement as part of her basic default package of rights. But in the case of the polluter, this is not so. In their default package of rights, polluters have at most a privilege – not a right – to pollute. Polluters do not have the right to pollute unless they have acquired an easement – an addition to the package of rights in land. Thus, there is no symmetry, because when the victim has the entitlement, it is a claim-right that tracks its basic package of rights in land. When the polluter has an entitlement to pollute, it is either a privilege and not a right, or it is a separately acquired easement – a right in the lands of another. Either way, something asymmetric is going on here.

III. ASYMMETRIC DELINEATION COSTS AND THE NATURE OF PROPERTY

The asymmetry of entitlements in property law is, I argue, a result of positive delineation costs. Some methods of delineating rights are less costly than others, and the less costly methods typically lead to "lumpy" entitlements of the asymmetric kind.

Consider first what delineation of legal relations would be like in a zero-transaction-cost world. In such a world, it would not matter at all what form entitlements took. To take two examples, A could have something like fee simple ownership of Blackacre, with the right to exclude the rest of the world from a column of space around the land as defined by the *ad coe-*

---

easement had been acquired. As one might expect, Coase was baffled by and rather hostile to this mode of thinking. *See* Coase, *supra* note 1, at 15 ("In deciding this question, the 'doctrine of lost grant' is about as relevant as the colour of the judge's eyes."); *see* Smith, *supra* note 3, at 965, 998.

[25] *See* HOHFELD, *supra* note 21, at 38-50.

lum rule.[26] Or, A could have an equivalent package of rights built from the ground up. That is, the right and privileges A has by virtue of fee simple ownership could instead be spelled out in terms of all the conceivable uses of Blackacre and all the possible competitors for those uses. A could have the right to use Blackacre for growing crops as against B (and C and D, etc.), have the right to parks cars on it as against B, C, etc., and so on. A would have the full fee simple package if these elaborately spelled out legal relations covered a relatively complete set of uses and duty holders. Both the list of use rights and the list of duty holders would be immense. Of course, looked at in this atomized way, A could just as well have a different bundle with only some uses and as against only some enumerated others. This ability to break notions like property down into their constituent parts leads one to wonder why the bundle A has could not be any other – usually smaller – bundle, as long as splitting the bundle in this way serves any beneficial end.[27] Thus, if B is someone who would like to enter Blackacre to delver a mobile home, why not give the mobile-home-dragging-right to B and avoid transaction costs?[28] The atomized bundle-of-rights picture of property makes the bundles the law provides look arbitrary and makes re-engineering the bundle seem attractive. And tailoring entitlements to capture any benefit not exhausted by transactions would make sense if the tailoring could be effected at little or no cost.

In a world of zero transaction costs, specifying A's rights as a right to exclude versus this articulated, atomized, "bottom-up" package (and its close relatives) would cost the same – nothing. If so, then there is no reason not to define property rights in the articulated extreme bundle-of-rights way. On the other hand, in the world of zero transaction costs there is no reason to define property rights in any particular way; in the zero-transaction-cost world the parties will bargain to the efficient result anyway. In this fictional world, there would be no need for a distinction be-

---

[26] The full statement of the maxim is *cujus est solum, ejus est usque ad coelum et ad inferos* (he who owns the soil owns also to the sky and to the depths). The maxim is routinely followed in resolving issues about ownership of air rights, building encroachments, overhanging tree limbs, mineral rights, and so forth, and is subject to certain limited exceptions such as for airplane overflights. *See* Brown v. United States, 73 F.3d 1100, 1103 (Fed. Cir. 1996); *see* Merrill, *supra* note 8, at 35-45 (discussing airplane overflights and other exceptions to *ad coelum* rule).

[27] *See, e.g.*, Arthur Linton Corbin, *Taxation of Seats on the Stock Exchange*, 31 YALE L.J. 429, 429 (1922) ("Our concept of property has shifted . . . . '[P]roperty' has ceased to describe any *res*, or object of sense, at all, and has become merely a bundle of legal relations—rights, powers, privileges, and immunities."); *See generally* THOMAS C. GREY, *The Disintegration of Property, in Property, in* 22 NOMOS 69 (J. Roland Pennock & John W. Chapman, eds., 1980); *see also* Merrill & Smith, *supra* note 3, at 365 (discussing this elaboration of the bundle-of-rights view).

[28] *See* Jacque v. Steenberg Homes, Inc., 563 N.W.2d 154 (Wis. 1997) (upholding a verdict of punitive damages of $100,000 on compensatory damages of $1 where the defendants moved a trailer home across the plaintiff's land and plaintiff refused all defendant's offers at least partly out of the mistaken belief that prescription might result).

tween property and contract: all "property" could be the result of bilateral bargaining between all conceivable competitors for the ability to perform any action whatsoever.[29]

In the positive transaction cost world, some shortcuts are in order. And one of the main methods of economizing on transaction costs is to avoid specifying legal relations in the Hohfeldian bottom-up manner. Delineating a right to use Blackacre for growing crops as against B is costly. By giving A the right to exclude, one can economize along several margins. First, the right to exclude need not refer to any specific use.[30] By giving A the right to exclude an unspecified group of others – all the rest of the world – A's interest in a wide range of uses, including growing crops, parking cars, etc. is protected without the need for the one delineating the right to know anything about – or even the existence of – these uses. Moreover, those who have to respect the right – the duty holders – need not know anything about these uses or about features of A.[31] The duty holder need only know to keep off. Finally, the one delineating the right need not know much about or even the identity of the duty holders; the right is to exclude the rest of the world. It is *in rem*. Of course from this baseline A might license B to enter Blackacre or even contract with B to exempt B from the general duty. But the baseline right to exclude with an exception for B is more economical than specifying all the right-duty pairs between A and all others individually.

In a sense, property law delegates to the owner both the choice among a wide range of (unspecified) uses and also the choice of possible modifications to the legal structure of rights and privileges over the owned asset. The degree of this delegation can be measured by how much the right to exclude serves as a shortcut over the full Hohfeldian bottom-up method of

---

[29] *See* Steven N.S. Cheung, *The Transaction Costs Paradigm*, 36 ECON. INQUIRY 514, 518-20 (1998) (arguing that in the zero transaction cost world there would not even be a need for property rights). Coase has agreed in principle with this observation. *See* RONALD H. COASE, THE FIRM, THE MARKET, AND THE LAW 14-15 (1990). At bottom, of course, this is simply a debate about the proper domain of the concept of "transaction costs." *See* Douglas W. Allen, *What Are Transaction Costs?*, 14 RES. L. & ECON. 1 (1991) (arguing that transaction costs are better defined as the costs of establishing property rights, in the economist's sense of a de facto ability to derive utility from an action, rather than narrowly as the costs of exchange).

[30] In a conceptual analysis, James Penner argues that in property exclusion (or gatekeeping) is fundamental to the right, and that the right protects the interest of people in using things. *See generally* J.E. PENNER, THE IDEA OF PROPERTY IN LAW (1997). I am suggesting here that like many concepts, the concept of property is a mental short cut and that one functional explanation for the concept is the large information cost savings of using the short cut as opposed to the direct Hohfeldian approach top protecting interests in use. *Cf.* JOHN LOCKE, AN ESSAY CONCERNING HUMAN UNDERSTANDING Bk. 3 Ch. 3 (Alexander C. Fraser ed., Dover Publ'n (1972) (1689) (arguing that only particulars exist but that having idea and word for every particular is beyond human capacity and would be useless even if it were possible).

[31] *See* PENNER, *supra* note 30, at 29; *see* Henry E. Smith, *The Language of Property: Form, Context, and Audience*, 55 STAN. L. REV. 1105, 1150-51 (2003).

delineating legal relations. In particular, consider the owner as a chooser among the possible uses of Blackacre. As already discussed, the right to exclude makes no reference to these uses, but, by installing the owner as a gatekeeper over the asset, the owner's interest in these uses is protected. The degree of delegation can be measured by the size of the "mismatch" between the right (to exclude) and the privileges of use that it indirectly protects. The greater the set of such use privileges implicitly protected by the right to exclude the greater the owner's range of discretion. Conversely, if the law makes detailed reference to uses and seeks to solve use conflicts between the owner and various neighbors or even between the owner and strangers, then the delegation is a lesser one; the law has removed from the owner some of the choice over uses and the choice over modifications of legal relations pertaining to those uses.

Thus, an *in rem* right, good against the world, is more than an arbitrary bundle among many other similar bundles. It is a key shorthand method of delineating rights that saves on the transaction costs of delineating and processing information about rights in terms of uses and users. Thus, positive transaction costs help explain why we have property at all instead of an elaborate system of contracting over much more specific use rights to resources and activities. It is because of positive transaction costs that we think in terms of things and especially in terms of *in rem* rights to exclude others from them – i.e. those rights known as *property*.

Shortcuts do have their costs. If rights are defined with very little reference to particulars like uses and users, benefits may be foregone. For example, Blackacre may be suited to having multiple people cultivating the crops or might be subjected to multiple uses as long as the two uses are constrained from conflicting too much. For example, some growing of crops and watching of (non-crop-eating) birds would be compatible as long as the birdwatchers took care not to trample crops and the farmers did not cut down too many trees. More precision in terms of who can do what when can be cost-effective in such cases: the benefits of adding precision beyond that in the basic right to exclude would pay the costs of the extra delineation and processing needed for the more elaborate rules. I call these more use-oriented rules examples of a governance strategy, as opposed to the basic exclusion strategy.[32] These governance rules come in many varieties. An off-the-rack legal version would be like some nuisance law and pollution regulation, in which a government actor determines the proper use, and enforces these rules on conflicting users. But governance schemes can and very often do arise through private contracting, as where neighbors or developers institute interlocking covenants, such as for the color of houses, residential use, etc. Or, proper use can be ensured through non-

---

[32] *See* Henry E. Smith, *Exclusion versus Governance: Two Strategies for Delineating Property Rights*, 31 J. LEGAL STUD. 453, 454-56, 467-78 (2002).

legal norms that are more detailed than the basic right to exclude.[33] Under what circumstances a neighbor is permitted to retrieve an errant child, pet, or toy is likely to be governed by norms rather than by formal law.[34] Consider too the elaborate but technically illegal system of norms governing the "entitlement" to a parking space that one has shoveled out after a snowstorm in many Chicago neighborhoods.[35] In such situations, the enforcement may be extralegal or even illegal, but the familiarity of a close-knit community will make the extra detail easier to achieve than in the case of formal legal governance regimes.

Returning to the notion of delegation, governance schemes involve some loss of discretion in the owner over the wide range of uses protected by the right to exclude. Judicial and other off-the rack legal governance regimes represent a direct withdrawal of the discretion from the owner.[36] By contrast, schemes of covenants or norms tend to involve a consensual surrender by owners of some of their discretion over the use of the owned asset, often in return for a similar surrender by other owners, to the mutual benefit of all. In agreeing to these use-restrictions, the owner exercises second-order discretion to transfer some (or all) of his rights and privileges to others.

IV. SELF-HELP AND THE DELINEATION OF PROPERTY RIGHTS

Self-help can be any one of a variety of rights or privileges. The choice between these different entitlements tracks closely the varieties of legal entitlements. Entitlements to self-help, like entitlements more generally, tend to rely on low-cost privileges and to piggyback on clumpy rights to exclude. Only in high stakes situations of great urgency do self-help rules become free standing rights.

A. *Varieties of Self-Help*

Consider first the distinction between self-help as a right and self-help as a privilege in the context of self-defense in the criminal law.[37] If A

---

33 *See generally*, ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); *see generally* ELINOR OSTROM, GOVERNING THE COMMONS (1990).

34 *See generally* ELLICKSON, *supra* note 33.

35 *See, e.g.*, Richard A. Epstein, *The Allocation of the Commons: Parking on Public Roads*, 31 J. LEGAL STUD. 515, 528-34 (2002); *see* John Kass, *Snowstorm's Charm Can't Stand Up to Law of Street*, CHI. TRIB., Jan. 5, 1999, at 3.

36 *See* Smith, *supra* note 3, at 1021-24.

37 *See, e.g.*, MODEL PENAL CODE § 3.04(1) (1962) (justifying use of force "when the actor believes that such force is immediately necessary for the purpose of protecting himself against the use of unlawful force by such other person on the present occasion"); *see* WAYNE R. LAFAVE & AUSTIN W.

unlawfully attacks B and B therefore has a privilege of self-defense against A, this means that A has no right against B that B not take reasonable self-help actions. B might have the privilege of hitting A, and A would not have the usual right not to be hit. This could come about in more than one way. For example, the aggressor A might have a general right to bodily integrity, but the law of self-defense removes this right, at least partially, as against B. Thus, when B hits A, B is not violating A's rights. The privilege of self-defense arises because B has a general privilege to act as long as it does not violate others' rights and the law of self-defense withdraws A's right against being hit by B. The general default privilege in B to act reasserts itself. Moreover, the original aggressor A has no privilege to act in self-defense against B (unless B's exceeds the allowed level of force), because B's self-defense attack on A is not unlawful as would be required for A to be allowed to exercise self-defense. On the view that self-defense is a privilege that is carved out of A's rights, B's general rights to bodily security avail without exception against A. If B uses excessive force, as when A pushes B and B draws a knife, A may then have some privilege to act in self-defense.[38] The law then makes an exception to B's rights of bodily security.

Another way for a privilege of self-defense to arise is for B to exercise the privilege of acting which is in turn protected by a right of exclusion. In self-defense, this would mean that if A invaded a physical space over which the law gives B the right to exclude, B could take a variety of actions within the space that harm A. However, because people's exclusion rights are routinely circumscribed by the rights of others not to be assaulted or killed no matter where they are, this way of thinking about self-defense does not add much in the case of violence.[39] But in the matter of lesser self-help actions, the fact that the privilege is one that is implicitly protected by a right to exclude can matter very much. Thus, if someone uses locks (but not spring guns) to defend property, the privilege of doing so is one of a great many that the owner can exercise behind the veil of the right to exclude.[40] There is no separately delineated "privilege to install locks;" it is a wholly implicit privilege protected by the right to exclude. The ability to provide for such a privilege implicitly saves on information and other delineation and enforcement costs. Conversely, the exercise of this and simi-

---

SCOTT, CRIMINAL LAW § 5.7 (2d. ed 1986) (discussing traditional approach to self-defense including requirement of imminence).

38 *See Id.* § 5.7(e).

39 At least these days. There was a time when actions taken to protect one's dwelling, including use of lethal force, were judged by a lenient standard; these days the tendency is to be less lenient to those engaged in self-defense within a dwelling (requiring a substantial risk to the defender), but still would not require the defender to flee. *See Id.* § 5.9; *see also Id.* § 5.7(f).

40 To be entitled to use force, the defender must reasonably believe that there is an immediate danger of unlawful entry or trespass (trespass or asportation in the case of personal property) and that it is necessary to use force to avoid the danger. *Id.* § 5.9(a).

lar self-help privileges is not a precondition for the ability to vindicate the right to exclude. There is no requirement that one lock one's house or car in order to sue trespassers and thieves.

By contrast, if B has the *right* to self-defense, this means that A has a corresponding duty of noninterference with B's exercise of his self-defense right. Thus, if B hits A in self-defense, A might have a duty not to ward off the blow, etc. Or, less likely, it could be that A must submit to being hit. But the duty does not normally extend that far. Indeed in such situations, A may withdraw and is encouraged to do so.[41]

Is the entitlement to engage in self-help a right or a privilege? One might think that it is a right, based on the fact that A is not allowed to respond to B's self-help with fresh violence of A's own. In self-defense, the original aggressor A has a duty not to use violence against self-helper B. But the source of this duty might be B's general right against violence against others in general, including A – rather than a special right of self-defense in B.[42] A probably does not have a duty to suffer the violence; if possible, A is allowed to (and would be well advised to) withdraw. A's lack of entitlement to respond to B's self-help with force could simply stem from B's general rights to be free from violence. Either way – B has a right to engage in self-help or B's general rights back up B's exercise of the privilege of self-help – there are limits to B's entitlement. If B exceeds the level of reasonably necessary force against A, then A can respond with force if necessary to prevent the excessive harm to A. This limit on self-help is consistent with a right or a privilege of self-help. If self-help is a right, B's right is so limited to reasonably necessary force, or the privilege of self-help in B is limited and then A's general rights to be free from physical harm kick in.

Another type of self-help, the law of necessity, features prominently in property law. Like self-defense, the law of necessity responds to situations of high urgency. Unlike self-defense, the law of necessity often centers on the entitlement of the one facing the necessity to have access and to use

---

[41] An aggressor who withdraws and communicates the withdrawal to the victim, "is restored to his right of self-defense." *Id.* § 5.7(e), at 460. On the view of self-help as a privilege, the original aggressor who withdraws is restored to his full right of bodily security and if the original victim further attacks him, the law makes an exception to the original victim's security rights, giving the original (withdrawn) aggressor a privilege of self-defense.

[42] Telling the two methods of establishing the right in B would not be straightforward. Consider a case in which B defending himself against A and A holds up a steel pipe in the path of B's fist. Probably A would be liable to B. Is this because B has a right of self help? Or is it that B in swinging his fist is acting in a way he is privileged to do – because of the absence of a right in A to be free from self-help violence – and for A to act in such a way as to cause B harm is tortious? Placing the steel pipe in the way of B's fist would be a legal cause of B's injury because B had an entitlement – privilege or right – to act. Compare someone who trips a pedestrian walking on the street with a steel bar.

property in ways that would otherwise constitute a trespass or conversion.[43] In the classic situation of necessity, one facing imminent harm, particularly to health or safety, is entitled to enter or use property of another. This self-help is sometimes referred to as an "incomplete privilege" because a private party in necessity may have to pay for any damage to the property.[44] In the famous case of *Vincent v. Lake Erie Transportation Company*,[45] the person in need was a ship-owner facing a danger in a storm. After discharging cargo at a dock the ship-owner decided not to unmoor because of a gathering storm. When the storm arrived, the ship was impelled against the dock and suffered damage. The court held that in light of the necessity the ship-owner acted reasonably and justifiably, but had to pay for the damage to the dock.[46] In the Calabresi and Melamed framework the dock is usually viewed protected by a property rule most of the time, but in situations of necessity the protection drops to that of a liability rule.[47] The one in peril can take and pay, but after the peril passes the property rule reasserts itself. Controversy in the liability rule literature has revolved around what kind of entitlement protection is afforded to the one facing necessity, here the ship-owner. In another leading case on the subject, *Ploof v. Putnam*,[48] a dock owner's servant unmoored a ship whose crew was trying to avoid a storm and as might be expected the ship was driven on the shore and the people and cargo on board were tossed into the water. The court held that the ship-owner had stated a case in trespass,[49] and I have argued elsewhere that this shows that the ship-owner had a right rather than a mere privilege to use the dock.[50]

Commentators have differed over the strength and scope of this right, with some arguing that the entitlement of the one facing the necessity (the ship-owner) is in turn protected by only a second-order liability rule, under

---

43 *See, e.g.*, LAFAVE & SCOTT, CRIMINAL LAW § 5.4; *see also* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 24, at 145-48 (5th ed. 1984).

44 *See* RESTATEMENT (SECOND) OF TORTS §§ 262 cmt. d, 263 cmt. e (1965) (noting that obligation to pay for damage arises in case of private but not public necessity); *see* RESTATEMENT OF RESTITUTION § 122 (1937) (describing "a duty of restitution for the amount of harm done" in one who derives benefits from an "incomplete privilege"); *see* Francis H. Bohlen, *Incomplete Privilege to Inflict Intentional Invasion of Interests of Property and Personality*, 39 HARV. L. REV. 307, 312-313 (1926); *see generally* Daniel Friedmann, *Restitution of Benefits Obtained Through the Appropriation of Property or the Commission of a Wrong*, 80 COLUM. L. REV. 504 (1980).

45 124 N.W. 221 (Minn. 1910).

46 124 N.W. at 222.

47 *See, e.g.*, Ian Ayres & J.M. Balkin, *Legal Entitlements as Auctions: Property Rules, Liability Rules, and Beyond*, 106 Yale L.J. 703, 710 (1996).

48 71 A. 188 (Vt. 1908).

49 71 A. at 189.

50 I argued that because the right here correlates with a duty in the dock owner to allow the crew to moor, this is a true claim-right in the Hohfeldian sense, as opposed to a mere privilege. Smith, Property Rules; *see also* WESLEY NEWCOMB HOHFELD, FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING 36-38, 71-72 (Walter Wheeler Cook ed., Greenwood Press, Inc. 1978 (1919).

which the dock owner could "retake" the entitlement to the dock but would have to pay damages to the ship owner.[51] Richard Epstein argues that during the peril, if the dock owner tried to unmoor the ship, the crew could defend with deadly force and the dock owner might be liable in trespass. If so, the ship's crew has the entitlement to the dock protected by a property rule, not a liability rule.[52]

But notice that this right, if it is a right, may not be a special right to the dock, but rather, the general right against unwanted contact. The ship-owner, being privileged to be on the dock, can use his general rights to be free from trespass to enforce his right to the dock. Or, it might be that the ship-owner has taken temporary possession of the dock and the right against trespasses is the right of a possessor against wrongful invasion. On this view, if the ship were not tied up and the dock owner put an obstacle in the way of the ship-owner from mooring, there would be no liability. Or, the ship-owner might have a right under which it could use some degree of force to barge in and take possession of the dock despite the owner's efforts. Thus, the ship-owner has some right, but it could be any of these three: (i) the right to be free from unwanted touchings by the dock owner, which is useful in helping the ship-owner exercise its privilege of using the dock; (ii) the right to use the dock, such that the ship owner has a duty to not to interfere (one variant on this would be that the right to use the dock arises once the ship-owner has gained possession of the dock but the ship-owner has no right, just a privilege, to gain possession of the dock); (iii) the right to use the dock with corresponding duties in the landowner to facilitate the use.

Whether actual possession by the one in necessity strengthens that person's claim to a resource, it does seem to be the case that the law of self-help does piggyback to a certain extent on notions of possession. This happens in two ways. One, which we have already discussed, is that possession gives a right to exclude (although one more contingent and less durable than the right to exclude conferred on full owners).[53] This right to exclude indirectly protects self-help measures taken by possessors to prevent invasions, such as erecting fences, installing locks, hiring guards, etc. Possession also limits the self-help privileges of others. In the context of docks and ships, the ship-owner is in possession of the ship and possibly the dock. Unmooring the ship would violate right of possessors to exclude.

---

51 *See* Ayres & Balkin, *supra* note 47, at 710.

52 Richard A. Epstein, *A Clear View of The Cathedral: The Dominance of Property Rules*, 106 YALE L.J. 2091, 2108-09 (1997). As Epstein points out, the owner could not "retake" the entitlement, but rather the property rule protection temporarily shifts to the boat owner because protecting life is more important than a refined "auction" of the dock.

53 The law provides for a rebuttable presumption that one in possession has a property right in it. *See, e.g.*, Russell v. Hill, 34 S.E. 640 (N.C. 1899). Making out a case of trespass requires that the plaintiff show she has possession; no showing of title is required. *Id.* at 640.

That possession is important in helping to define the scope of entitlements to self-help also helps explain why self-help repossession has been such a thorny issue in the law. The law has become more hostile to efforts at self-help repossession, particularly in real property.[54] In the landlord tenant context, both tenants and landlords have aspects of the right to exclude.[55] The tenant has the present right to exclude third parties and limited rights to exclude the landlord. In landlord-tenant situations, the owner has delegated the right to exclude for a limited period of time to the tenant. To the rest of the world the tenant appears, like owners, to be exercising the right to exclude. The landlord has the future right to exclude third parties, and usually has limited privileges to enter for purposes of repairs and to show the premises to prospective tenants.[56] Tenants have a wide range of use privileges protected by the right to exclude, and many of these include self-help to impede invasions. When a landlord tries to repossess, tenants can be expected to resist. Instead of delineating the boundaries of the tenant's privilege to resist, the modern trend is to force the problem into a judicial forum, where the respective rights of the parties can be determined.[57] The deference to self-help is heavily based on exclusion, and when possession and ownership are separated, the law is less deferential to the owner's right to exclude.

The lesser degree of deference to self-help by owners not in possession can be interpreted in several ways, all of which are consistent with the information-cost theory. First, information costs are lowered by deferring to efforts by those in possession – usually but not always owners – to keep the gate over the asset in question. Second, in the bailment and landlord-tenant situations, there are multiple parties with some piece of the right to exclude. This leads to conflict and complication. The law can either side with one or the other, or it can regulate the conflict in the interest of third parties. Where self-help tends to a breach of the peace, the law increasingly steps in and requires owners not in possession to use legal process. This is increasingly true in the context of real property (landlord-tenant), but courts are still somewhat deferential to self-help repossession in the case of personal

---

54 *See* Douglas Ivor Brandon et al., Special Project, *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845, 950-53 (1984).

55 *See* 2 Richard R. Powell, POWELL ON REAL PROPERTY § 16B.02[2] (Michael Allan Wolf, ed., 1949) ("Once initial possession is established . . . it is clearly the tenant's responsibility to ward off trespasses."); *see also* Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 831-32 (2001).

56 *See* 1 MILTON R. FRIEDMAN, FRIEDMAN ON LEASES § 4.202, at 95-100 (4th ed. 1997). An attempt to override this feature of leases and give the landlord unlimited privileges of access would probably be held to contradict the nature of a lease. 3 *id.* § 29.303, at 1658.

57 *See, e.g.*, Berg v. Wiley, 264 N.W.2d 145 (Minn. 1978); WILLIAM B. STOEBUCK & DALE A. WHITMAN, THE LAW OF PROPERTY § 6.80 (3d ed. 2000).

property.[58] As long as the exercise of the privilege of self-help to repossess personal property does not tend to breach of the peace, the courts will generally allow it. Notice that in the case of personal property self-help is pursued pursuant to a privilege rather than a right.[59] One who owns a car subject to a lien that secures a loan in default would be liable to repossession and may have no right to exclude, but such a person has no duty to allow the repossession either. Thus, if the possessor of the car locks the car in her garage, the repossessor has no right to break in. In some cases, courts will not allow the repossession if the possessor of the car objects vociferously enough;[60] the thought is that if the repossession proceeds beyond this point, there is a heightened risk of violence or other breach of the peace.

B. *Self-Help and Degrees of Delegation*

The law's various approaches to self-help reflect the costs and benefits of delineating entitlements. In this section, I outline a simple theory of delineation cost and draw out some implications for self-help.

As already mentioned, entitlements do vary more than expected on the symmetry-based, conventional law and economics approach. Entitlements vary systematically in a way that reflects some very basic costs and benefits of delineation. These costs and benefits, although often overlooked in the search for Coasean symmetry, are important and widespread, and are at least partially internalized to those actors – private parties, lawmakers, and judges – who have to set up the rights and enforce them.

Consider again the so-called entitlements to pollute. When residents have the right to be free from pollution, they are vindicating the right to exclude from boundaries as defined by the *ad coelum* rule.[61] The resource conflict is assimilated to a package of rights defined by the exclusion strategy; the signal for whether the right has been violated is largely a matter of

---

[58] *See* Revised U.C.C. §§ 9-609, 9-602 (2003); 2 GRANT GILMORE, SECURITY INTERESTS IN PERSONAL PROPERTY § 44.1, at 1212 (1965). Importantly the U.S. Supreme Court has held that repossessions under the Uniform Commercial Code do not trigger due process. Flagg Brothers, Inc. v. Brooks, 436 U.S. 149 (1978). This means that creditors have preferred to use security interests rather than actions like replevin that do implicate due process, and thus owners of personal property subject to liens are less protected under the U.S. Constitution in situations involving repossession, in which creditors have more discretion than under statutory remedies like replevin and garnishment.

[59] This is often overlooked. Despite being called a "right" of self-help, decisions that allow for self-help only as long as there is no objection from the debtor set up a privilege, not a right, of self-help. *See* Hester v. Bandy, 627 So. 2d 833 (Miss. 1993); Curtis Nyquist, *Teaching Wesley Hohfeld's Theory of Legal Relations*, 52 J. Legal Educ. 238, 241-42 (2002).

[60] *See, e.g.*, Williams v. Ford Motor Credit Company, 674 F.2d 717 (8th Cir. 1982).

[61] *See supra* note 26 and accompanying text.

boundary crossings by physical objects.[62] The exclusion strategy is low cost but also low precision. It is the cost effective strategy for prevention of gross invasions and allows the owner to act as gatekeeper. Exclusion effects a delegation to the owner and is reflected in the radical mismatch – the lack of precision – in the signal used to delineate the right and the uses of the resource that the right protects. This, in the case of the owner of Blackacre, the owner's right is protected by common-law actions like trespass that rely on the signal of boundary crossing; this signal is typically over-inclusive when regarded in the light of the uses that it is protecting. Not everyone who has crossed the boundary and is present on Blackacre is harming uses like the growing of crops.

Further precision requires signals more narrowly tailored to use, in what I call a governance strategy. A wide variety of actors and institutions can supply entitlement structures using a governance strategy. First, the owner as gatekeeper might contract with others over the use of the resource. If this is done, then free-standing rights like easements to pollute can be drawn up by the parties and enforced. Second, the law can provide these governance rules directly in centralized fashion, employing off-the-rack tailored signals of use. Some nuisance law and much of zoning law do exactly this: rules for proper use are imposed on owners, either as defaults or mandatory rules. The signal or trigger for liability tracks notions of proper use more closely than signals based on boundary crossings. Consider a rule permitting some level of noise or odors but nothing in excess of that level, or a rule that allows a given use as long as it is valuable enough. The rules of nuisance can themselves, transaction costs permitting, be altered through negotiation between affected parties; anti-pollution environmental laws cannot. Finally, it should be noted that norms may supplement the basic exclusion regime with rules of proper use based on tailored signals. The governance strategy achieves the benefits of higher precision, which usually involve use by multiple parties with access (conditioned on proper use), but this extra precision is achieved at higher cost.

Two issues present themselves as to which strategy is best in a given situation. First, we have to ask where the collection of marginal cost curves of delineation intersects the marginal benefits of delineation.[63] But ideally, marginal cost here is the cost of adding precision to entitlements using the least cost method of delineation.[64] At low levels of precision, this is likely to be exclusion, but at higher levels of precision this is likely to be governance.[65] On top of this basic picture, there are different suppliers of the two strategies, particularly in the case of governance. If optimality is to be

---

62 This is the approach taken in trespass law and in a great deal of nuisance law. *See* Smith, *supra* note 3.

63 Smith, *supra* note 32, at 474-78.

64 *Id.* at 476-77.

65 *Id.* at 474-77.

achieved, the law should not supply rules of proper use unless (a) the benefits cover the costs, and marginal benefit equals marginal cost (total net benefits are maximized), (b) exclusion would not be more cost-effective, and (c) no other supplier can achieve this result at lower cost. Normatively speaking, this leaves a narrow band for off-the-rack governance rules.

Furthermore, this simple framework also provides some normative and, under certain assumptions, positive perspective on changes in property rights systems. Movements of either the marginal benefit curve or the marginal cost curve (or its component curves) for the various entitlement delineation strategies can have effects at the margin. At the most macro level, increases (decreases) in marginal benefits of precision or decreases (increases) in marginal cost of delineation will lead to more (less) delineation of entitlements. This is the basic Demsetzian story that property rights will emerge to internalize externalities.[66] With some modification, we can accommodate a more pessimistic version in which the actors deciding whether to engage in property rights activity face benefits and costs that do not coincide with social benefit and cost.[67]

The framework also allows us to derive some propositions about the relative reliance on exclusion and governance. For example, governance rules rely more than do exclusion rules on personal information and face-to-face interaction. So an increase in the costs of face-to-face negotiation will cause a greater increase in cost for the governance strategies than for the exclusion strategies. Thus, in these situations we would expect a shift from reliance on governance to a reliance on judicially determined governance or even exclusion.

The costs of delineation will also increase when the uses to which an asset might be put become more multiplex, more uncertain, and generally harder to measure.[68] If the benefits of delineation did not also increase – more on this in a moment – then we would expect one or both of the following: a decrease in property rights activity and a shift in emphasis from governance to exclusion, at least as far as off-the-rack law goes. For example, one argument for broad rights in intellectual property is that the difficulty in developing information about particular uses of information points towards the functionally broad rights typical of patent law.[69]

The problem in many dynamic settings is that uses become more multiplex and uncertain *for the same reasons* that they become more valuable

---

66 Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. PAP. & PROC. 347 (1967). Increased delineation of entitlements can take the form of more and stricter governance rules, not just more exclusion. *See* Smith, *supra* note 32, at S470-83.

67 *See, e.g.*, Stuart Banner, *Transitions Between Property Regimes*, 31 J. LEGAL STUD. 359 (2002); Saul Levmore, *Two Stories about the Evolution of Property Rights*, 31 J. LEGAL STUD. 421 (2002).

68 *See* Henry E. Smith, *Intellectual Property as Property: An Information Cost Approach* (Feb. 7, 2004) (unpublished draft, on file with author).

69 *Id.*

and so more appropriate as the subject of entitlements. In other words, the marginal cost and marginal benefit of delineation and enforcement activity shift outward. Which curve (marginal benefit or marginal cost) shifts out more will determine the direction of change. Thus, if a resource becomes more valuable because of multiplex uses, but this increase in value raises the marginal benefit of entitlement supply more than the associated increase in the marginal cost of contracting, then there will be a tendency to contract for precise rights of the uses of the resource. Increases in intellectual property licensing may be an example. Likewise, if contracting is very costly but additional off-the-rack rights definition is cost-effective, we may get, for similar reasons (MB shifts greater than MC) additional articulation of the legally defined bundle of rights. Much depends on the extent to which officials designing and implementing entitlements respond to considerations of cost and benefit. This could be either because judges or other actors face information costs similar to those facing duty holders, or in some cases those who benefit from the greater articulation of rights would be organized enough to have their way in the legislative arena. An optimistic view would hold that some compulsory licenses in copyright fit this description.[70]

My thesis is that much of recent controversy in intellectual property, and especially where intellectual property and self-help meet, is the result of simultaneous increases in the marginal benefits and in the marginal costs of entitlement delineation facing officials. It is much less clear that private parties face increased costs of delineation; technological change is at the same time lowering the cost of contracting and of using digital self-help, to which I return below, and is also lowering the costs for intruders. Nevertheless, within the set of strategies used by the law to delineate entitlements, if uses are more costly to delineate but private contracting on the base of the exclusion strategy is still viable, we should expect an emphasis on exclusion in the law as technology advances.

Ultimately, of course, the size of these various effects is an empirical question, but I will argue that some of the grossest types of costs and benefits cause the law's approach to self-help to reflect, in a rough way, the economization of delineation costs – even when self-help seems to be at odds with the basic entitlement structure. More tentatively, I argue that recent developments reflect changes in the costs and benefits of using the exclusion and governance strategies in delineating entitlements – including entitlements to self-help.

---

[70] *Id.* A more obvious example would be the history of the law's response to owner's claims to exclude airplane overflights. *See, e.g.*, PROSSER & KEETON ON TORTS, *supra* note 43, § 13, at 79-82; Colin Cahoon, *Low Altitude Airspace: A Property Rights No-Man's Land*, 56 J. AIR L. & COM. 157 (1990).

The law's approach to self-help depends in part on the degree of delegation to owners of choices over uses, and the extent of this delegation in turn depends on delineation cost. First, the difficulty of separating out and measuring uses points toward exclusion rather than governance (as long as having some entitlement is appropriate in the first place). When it comes to self-help, the boundaries used in the exclusion strategy reflect delegation to owners and the law of self-help tends to track this choice. Thus, the law pays great deference to activities taken by owners, such as fencing, that are exercises of a privilege to act in a wide and unspecified set of ways. Conversely, self-help that requires the one engaging in it to cross boundaries, will receive much less deference. Thus, the common-law privilege to abate a nuisance on another's land is hedged about with many qualifications. Self-help abatement of a nuisance is only allowed after notice is given to the nuisance-causing landowner, the one abating the nuisance may use no more than reasonably necessary force, and the need to remove the nuisance must be urgent.[71]

Second, the higher the stakes involved in a given use, the more likely that a narrowly carved out privilege or even a stand-alone right will be cost-effective. Thus, as the benefits increase, it makes more sense to carve out a privilege (for example, to emit some odors), or even more expensively, to create a stand-alone right (like an easement). Consider the carving out of privileges of self-help. Here someone has a right to exclude, but the law partially withdraws this right by allowing someone else to exercise a privilege (which would have been a violation of the pre-carving right). For example, the owner of Blackacre has a right to exclude trespassers and thieves, but in situations of necessity, the owner has a Hohfeldian "no right" that corresponds to a privilege, held by certain others in danger, to enter and use the resource.

If the situation involves high enough stakes it may make sense to incur even greater delineation costs. One way would be to delineate a stand-alone right to engage in self-help. This would be something like an easement to engage in self-help, under which the other party would have a duty not to interfere with the self-help, or in the most costly version would have a duty to facilitate the self-help. The right of one facing necessity would be an example, although the scope of this right is often unclear.

It should be said that the law contains very few positive duties to act, and even fewer duties to act affirmatively are cast on the world at large.[72] In the property context, only doctrines of lateral support and party walls

---

[71] *See* PROSSER & KEETON ON TORTS, supra note 43, § 89, at 641-43. There are many parallels here to the law of necessity and of self-defense.

[72] *See, e.g.*, A.M. Honoré, *Rights of Exclusion and Immunities Against Divesting*, 34 TUL. L. REV. 453, 459 (1960) ("[T]here appears to be no instance, either in the Anglo-American or continental lists, of a right protected by a claim that persons generally should perform something."); Merrill & Smith, *supra* note 55, at 788-89.

prominently exhibit these positive duties. Note that, unlike with the classic *in rem* property rights, the parties in these situations of lateral support and common walls are few and readily identifiable, and the message to these parties is relatively simple.[73] Likewise, returning to the law of necessity, the relation between the one in necessity and a given owner is a special one and does not require affirmative acts on the part of the owner. Situations of legally sufficient necessity are rare.

All sorts of other stand-alone rights to engage in activities do exist, but these tend to be privately negotiated easements and covenants. And, the more these interests impact third parties the less information the law allows to be packed in them: the set of easements, which are rights *in rem*, is more standardized than contracts between two parties (and possibly their successors).[74] What we do not find are bundles of judicially created easements to capture the benefits of tailored use, as one might expect on the Coasean approach.

When the law does supply precision in entitlements, including those regarding self-help, it tends to carve out privileges from others' pre-existing rights or, more rarely, creates narrow stand-alone rights. "Carving out" privileges, especially creating stand-alone rights, reflects less deference to owners and a shift from exclusion to governance. We should only expect this where the stakes are high and private parties cannot supply governance more cost-effectively themselves. Another method of withdrawing deference is by conditioning the exclusion strategy on self-help acts by owners. In the case of physical property, we find little use of this procedure, but it forms the basis for trade secret law. Or, the law can forbid certain self-help actions; this may or may not require much separate delineation if the right of another to be free from self-help is closely related to general regulations against use of violence, etc.

In summary, varieties of self-help and their place in the scheme of entitlement delineation can be thought of as a system of increasingly specific and costly rules, where more specific rules displace more general rules:

1. Basic background: Presumptive privilege to act.

2. Rights to exclude (exclusion strategy), which implicitly protect a wide range of interests in use (privileges) without the need for these to be spelled out.

3. Exceptions to the right to exclude, allowing (stage 1) privileges to reassert themselves. (Obvious cases include airplane overflights, *de minimis* non-trespassory invasions, necessity, and the more borderline cases in nuisance).

---

[73] *See* Charles E. Clark, Real Covenants and Other Interests Which "Run With The Land" 144-69 (2d ed. 1947); Merrill & Smith, supra note 55, at 789 & n.53.

[74] *See* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1, 16-17 (2000).

4. Freestanding narrow rights (rarely off-the rack, virtually never casting affirmative duties on the world at large; sometimes separately negotiated as with easements and other servitudes).

Privileges indirectly protected by broad rights are the least costly but least tailored, and reflect the greatest degree of delegation to owners. Privileges of self-help are indirectly protected by the right to exclude, and the law very deferentially regulates only the limits of this kind of self-help, in the way that tort law regulates people's activities in general. Other less deferential approaches are used in higher stakes situations. A common method for dealing specifically with self-help is to define privileges of self-help directly by carving out an exception to another's rights. If so, general privileges to act reassert themselves *without any more need for delineation.* The most fundamental baseline is the right of people to engage in an activity unless otherwise prohibited. So, most liberties need not be separately defined. The price is that such privileges of self-help are weak in the sense that there is no legal guarantee that the self-help won't be defeated by the actions of others pursuing their own liberty. If the stakes are high enough – as they often are in situations of necessity – we should expect some shift toward more regulatory, less deferential but more costly approaches involving setting up special rights of self-help. Thus, an entitlement to self-help can be a stand-alone right of varying strengths; it might require another party to refrain from interfering with the self-help. Stronger rights would add more parties (making the right of self-help more of an *in rem* right) and would require more specific affirmative actions on the part of the duty holders.

V. DIGITAL SELF-HELP

Controversies surrounding self-help in the digital arena, including trespass to websites, digital rights management, and copyright fair use, raise questions of entitlement delineation. Most of the recent commentary on this issue has been very hostile to importing notions from the law of tangible property.[75] It is said that these notions reflect absolutist and hyper-

---

[75] *See, e.g.*, LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 161 (2001) (contending that enclosure propertizing information by media and software companies is stifling innovation in the New Economy); SIVA VAIDHYANATHAN, COPYRIGHTS AND COPYWRONGS: THE RISE OF INTELLECTUAL PROPERTY AND HOW IT THREATENS CREATIVITY (2001); Tom G. Palmer, *Are Patents and Copyrights Morally Justified? The Philosophy of Property Rights and Ideal Objects*, 13 HARV. J.L. & PUB. POL'Y 817 (1990) (arguing for a private property system that does not recognize copyrights or patents); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 386-412 (1999) (arguing against expanding copyright at the expense of the public domain); James Boyle, *The Public Domain: The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33 (2003) (arguing against increased propertization of intellectual property law at

formal notions of property and wooden applications of inappropriate analogies.[76]

I will argue that, like the realist critiques of traditional property law, this new conventional wisdom in the law of information goods gets the picture half right. The exclusion strategy is not perfect: it is crude and its hallmark is its lack of tailored fit to the particular uses to which a given resource might be put. As in the context of tangible property, additional, more tailored governance rules might be adopted, either through the efforts of private parties, or though official provision of off-the-rack rules and regulations of proper use. Like the realists in the realm of tangible property, the new commentators are skeptical that private parties can do much to supplement exclusion in desirable ways.

What the realist critique in tangible property and the new commentary in intellectual property both leave out is the flip-side of these foregone benefits in the exclusion strategy, namely the costs of various ways of setting up legal entitlements. If rights are justified in the first place, the question is their shape and extent. Much of the recent commentary in intellectual property does not advocate eliminating rights in intellectual property, but does propose much weaker and narrower rights than in current law; the controversy is a matter of degree.

One facet of the inquiry, then, has to be which strategy for defining rights is most appropriate. If the choice for exclusion versus governance is based primarily on benefits, the choice is clear: governance looks better because it can capture the benefits of multiple uses. For example, if delineating rights were costless, A could have rights to farm Blackacre and B could have rights to hunt there, or perhaps even grow vegetables in certain areas. Any combination of uses could be managed at zero cost. Exclusion rules, without more, do not do this. Likewise with information goods, the non-rival nature of information makes the costliness of exclusion in foregone benefits quite salient.[77] Even if information goods are non-rival, the inputs to creating and commercializing information products are rival,[78] and here, as in the case of tangible property, tailored governance rules, if they were costless, would do the job better. At the very least, rules of use could

---

the expense of the public domain); Mark A. Lemley, *Romantic Authorship and the Rhetoric of Property*, 75 TEXAS L. REV. 873, 985-904 (1997) (criticizing trend of propertization of intellectual property law, including the coinage of the phrase "intellectual property"); Jessica Litman, *Breakfast with Batman: The Public Interest in the Advertising Age*, 108 YALE L.J. 1717, 1725 (1999) (lamenting inexorable pressure to treat things of value as property).

[76] *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); Mark A. Lemley, Place and Cyberspace, 91 CAL. L. REV. 521 (2003); Dan L. Burk, The Trouble with Trespass, 4 J. SMALL & EMERGING BUS. L. 27 (2000).

[77] *See* the sources cited in *supra* note 75.

[78] *See, e.g.*, Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265, 275-76 (1977) ("There is, however, a scarcity of resources that may be employed to use information, and it is that scarcity which generates the need for a system of property rights in information.").

involve charges for different users, or the government could provide public subsidies for the "proper" use of inputs for creation and commercialization of information-based products, again at no cost.[79] Exclusion could not do better and would probably do worse if there is even one value-increasing transaction that does not occur under exclusion.

But one of the main advantages of exclusion is its low cost, and its cheapness is inseparable from its lack of fit with notions of proper use. By using a signal that defines a right that only indirectly protects a wide range of unspecified use privileges, the exclusion strategy achieves two things at low cost. It protects the owner's expectations and allows the owner to coordinate with others on proper use. The well-known downside of rights to exclude – that owners might use their holdout power or transaction costs might impede valuable uses – must be compared with the advantages of exclusion strategies in terms of saved delineation costs, especially information costs. Before an official scheme of entitlements based on proper use – an off-the-rack governance strategy – can make sense, it must be the case both that the problems of foregone multiple use are worth the trouble *and* that a combination of exclusion and privately instituted governance cannot do better. To go back to an analogy to real estate, much of the commentary on information entitlements assumes that something like nuisance and zoning is preferable to trespass. It might be, but the cost question has to be answered first. This cost question is an empirical one, and my main point in the following is to point out that we cannot conclude that the exclusion strategy is inappropriate until we can answer – even at the level of guesswork – the question of costs as well as benefits. Because the cost side has been so neglected, I suspect that the best guess given the current state of our knowledge is that exclusion is more warranted than conventional realist-style wisdom would have it. But these latter conclusions are more tentative and I will also point out places where an information-cost theory suggests suspicion of the increased propertization in intellectual property and related areas.

A. *Digital Trespass*

Perhaps the sharpest controversy over the application of what I am calling the exclusion strategy to cyberspace is the question of trespass to

---

[79] Many proposals to replace intellectual property with prizes or to employ liability rules have this flavor. On prizes, see Steven Shavell & Tanguy Van Ypersele, *Rewards Versus Intellectual Property Rights*, 44 J.L. & ECON. 525 (2001); Michael Abramowicz, *Perfecting Patent Prizes*, 56 VAND. L. REV. 115 (2003). For other tailored entitlement proposals, see, e.g., Ian Ayres & Paul Klemperer, *Limiting Patentees' Market Power Without Reducing Innovation Incentives: The Perverse Benefits of Uncertainty and Non-Injunctive Remedies*, 97 MICH. L. REV. 985 (1999); Michael Kremer, *Patent Buyouts: A Mechanism for Encouraging Innovation*, 113 Q.J. ECON. 1137 (1998).

websites. Even the notion that cyberspace is a place is said to reflect unfortunate and unwarranted analogies to physical space.[80] On this view, because of the non-rival nature of information and the low costs of communication and interconnection in cyberspace, notions from property law that seem to presuppose a place over which rights can be defined are inherently counterproductive. Many intellectual property commentators draw the conclusion that exclusion does more harm than good, and, for them, notions of trespass are Exhibit A.

Without claiming that there are no new issues here, I should point out that this whole question can be framed in a way that makes it sound very much like controversies that arise in the law of tangible property. One of the central issues in property law is to what extent exceptions should be made to rights to exclude. Should they be softened in favor of those who would like to use the property out of necessity, convenience, or to further some other social policy? In other words, if giving the owner a right to exclude others from a resource delegates to that owner a choice among uses of the resource, then various exceptions to the right to exclude reflect a partial withdrawal of that delegation.[81] If exceptions are made, how much does an owner have to stay out of the user's way or even to facilitate others' use?

One view in the digital arena is that rights to exclude should be very minimal indeed. One could say that by connecting up a computer or a network to the larger Internet, one has joined a large commons.[82] Then the question is how some central actor, either through standard setting organizations or the government, or some more spontaneous evolution of norms, or technological fixes, can prevent resource conflicts within this overall commons. Others point out that scarcity still governs some aspects of cyberspace and that it is run on equipment that is subject to the law of personal property.[83]

In actual cases that have arisen so far, the issue is usually defined more narrowly. When someone sends unwanted e-mail or accesses a website in a manner forbidden by the owners of the website (the owners or authorized users of the home computers hosting the website), should this count as a

---

80 *See supra* note 76.

81 *See* Smith, *supra* note 3, at 1021-45.

82 *See, e.g.*, Burk, *supra* note 76, at 48 ("But at the same time, the act of joining a local network to the great 'network of networks' that comprises the Internet indicates a desire to take advantage of the positive network externalities of the digital commons."); *see also* Lessig, *supra* note 75.

83 *See, e.g.*, Daphne Keller, *A Gaudier Future That Almost Blinds the Eye*, 52 DUKE L.J. 273 (2002) ("The ambiguity regarding property rights in the Internet's physical . . . . is rooted in one of the most confounding questions Lessig raises: how can a single, coherent property regime be tailored to account both for the Internet's value as a communicative platform for potentially endless cultural, political, and technical innovation and as a finite, exhaustible set of physical objects created by human investment?"); James B. Speta, *A Vision of Internet Openness by Government Fiat*, 96 NW. U. L. REV. 1553, 1562-67 (2002) (discussing advantages of private property in the physical infrastructure of the internet).

trespass at all, or should it be treated as a potential trespass to chattels (personal property)? And if there is a potential trespass, what counts as the harm to the chattel? Or should a trespass to a website not require substantial harm but merely a tangible invasion, as in trespass to real estate?[84] From one point of view, the answer is obvious; computers are personal property not real estate. But contrasted to this external point of view is an internal point of view in which the user feels as if she were "visiting" a website.[85] The website has a fixed location – an "address" – and is relatively stationary and easy to locate.

A number of recent cases have dealt with the problem of unwanted e-mail. In most of these, there was an allegation that the unwanted e-mail overloaded or slowed down the network.[86] In these cases, courts have allowed the plaintiff to proceed on a theory of trespass. One might view the trespass as a trespass to chattels – the overloaded computers and disk space. Some authority (notably the Second Restatement) requires for trespass to chattels that the defendant cause harm by interfering with the owner's use.[87] By contrast, trespass to real estate does not require a showing of actual harm. But the cases involving large quantities of e-mail have found the requisite harm, making a trespass to chattels claim available on any theory.

One recent case raised the issue of the difference between the two approaches to trespass. In *Intel Corp. v. Hamidi*,[88] a disgruntled former employee sent several e-mails to a long list of current Intel employees criticizing the company. Hamidi informed the individual employees that he would stop sending messages to any employee who objected. After asking Hamidi to stop and taking unavailing self-help measures to stop Hamidi's e-mail, Intel sought an injunction on a trespass theory.[89] The majority treated this as a trespass to chattels case and required actual harm. There was no evidence that the quantity of Hamidi's e-mails caused Intel's network any problems, and the majority held that there was no trespass.[90] The majority rejected an application of a real estate style trespass under which actual harm would not be required. Commentators as *amici* lined up as one might

---

84 *See* Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73 (2003).

85 *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003).

86 *See, e.g.*, eBay, Inc v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1060-63 (N.D. Cal 2000); America Online, Inc. v IMS, 24 F. Supp. 2d 548, 550 (E.D. Va 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D.Ohio 1997).

87 *See* RESTATEMENT (SECOND) OF TORTS § 218 (1965).

88 71 P.3d 296 (Cal. 2003).

89 Hamidi originally plead nuisance as well, but voluntarily dropped the claim when the district court was about to grant it summary judgment. Intel Corp. v. Hamidi, 71 P.3d at 301-02. For a discussion of how nuisance might apply, Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 646 (2004).

90 71 P.3d at 311.

expect.[91] Those who believe we have too much intellectual property and that property is an illegitimate source of analogies were in favor of finding no trespass (or at least requiring actual harm), and those more pro-property commentators were in favor of a real estate analogy.

In the *Hamidi* case, it is worthwhile to notice how the entitlement structure that the majority chooses illustrates the hidden asymmetries I discussed earlier. As Justice Mosk pointed out in dissent, Intel did use self-help against Hamidi's e-mails, and the majority found that permissible; Hamidi therefore had no *right* to have the e-mails reach the employees through Intel's system.[92] 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.[93] 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.

In the case of real property, the law of trespass is particularly simple. Non-accidentally causing a physical object to cross a boundary into the column of space surrounding land, as defined by the *ad coelum* rule, is a trespass.[94] More ethereal invasions by odors or sounds are nuisances if they are legally redressable at all. Trespass to chattels is also a bright line rule but in some formulations does differ in terms of what harm is required. Trespass to chattels is sometimes said to require that the trespasser cause some actual damage, but there can be disagreement (as there was in *Hamidi* between the majority and the dissents) as to what type of harm is required: is physical damage to the chattel (or some related chattel) required or harm to a related interest of the owner?[95]

In terms of the information cost theory, one can make some sense of this difference between trespass to land and trespass to chattels. First of all, in terms of which signals to use to define entitlements, in the case of land the boundary is one that can be crossed. The crossing of a boundary is a low-cost signal that sweeps in a wide variety of uses into its protective fold.

---

91 *Id. at* 309-11 (contrasting views of Richard Epstein on the one hand and those of Mark Lemley, Dan Hunter, Lawrence Lessig and other law professors).

92 *Id.* at 331 ("By upholding Intel's right to exercise self-help to restrict Hamidi's bulk e-mails, they concede that he did not have a right to send them through Intel's proprietary system.").

93 *See* Calabresi & Melamed, *supra* note 10, at 1116; *see also supra* notes 19-23 and accompanying text.

94 *See supra* note 26.

95 Intel Corp. v. Hamidi, 71 P.3d at 302-08; *Id.* at 322-25 (Brown, J., dissenting); *Id.* at 326-29 (Mosk, J., dissenting).

In the case of things (other than real property), this is less clear because the problem with someone violating property rights is usually not the object has been punctured. What is the "boundary" here that is analogous to the boundary in the *ad coelum* rule? One might say that there is some region of space around the object but this is likely to vary by object and by context. And a flat rule that no one can touch another's owned object is likely to be vastly over-inclusive; imagine someone trying to fetch his umbrella out of an umbrella stand at a restaurant without touching any of the others. We are forced to recognize that most such touchings would be *de minimis*. What is not *de minimis* is a touching or other use that inflicts some damage to the owner as user. It is not that we have suddenly left the exclusion strategy and have decided, governance-style, to prescribe proper use of chattels through the law of trespass; on the contrary the actual harm is functioning as the low-cost signal for the violation (i.e. a trigger for liability) of a gatekeeper right. It is simply the nature of the resource here that forces the use of a different signal than in the case of real property.

To this can be added that, traditionally, it was thought that the uses of land were particularly hard for outsiders to evaluate, making a "deferential" signal all the more important in the case of land. The *ad coelum* rule, by making essentially no reference to use whatsoever, achieves a high degree of deference to owners in their actual and planned uses of real estate. No harm need even be shown.

How does all this richer theory of entitlement delineation apply to controversies over resources in cyberspace? It suggests factors that have received less than due attention. We have to decide the degree of delegation to owners and which informational signal achieves this degree of deference at reasonable information cost, not least the costs to third parties in deciphering the entitlements. Thus, if we are worried that websites can be put to many uses, and we do not want owners to have to justify their decisions to outsiders, a more deferential signal, perhaps even the *ad coelum*-style approach not requiring actual harm, is in order. Part of what determines information cost would be the nature of the resource. How difficult would it be to define a spatial-type signal of boundary crossing in the case of websites? Or would such a signal lead to the over-inclusion of *de minimis* intrusions? I will suggest that much depends on the costs of furnishing notice to duty holders.

These third-party information costs of different strategies for delineating and enforcing entitlements depend in part on the nature of the resource in question. In the case of land or chattels, sending a message to potential intruders is rather difficult. Signs and written notices are the main devices, but these are costly to provide. In the case of websites, one can easily provide for a page of terms that condition further access on agreement to those terms. The greater problem is ensuring that users read such notices and that they are not too ambiguous. The problem becomes essentially a contractual one. I take up the question in the next section. In the case of unwanted e-

mail it is difficult for someone contemplating sending a message to know whether the e-mail might be unwanted. The situation is somewhat like an unwanted telephone call.

It should be noted that even in the case of real estate, the exclusion strategy does allow some invasions to count as *de minimis*. As already mentioned, airplane overflights are not trespasses. Nor is using the electromagnetic spectrum to send signals over land a violation of the *ad coelum* rule. Nor is sending electricity to a toaster "trespass to toasters."[96] It is thought that such invasions are too insignificant and mutually beneficial to count as trespasses. On the other hand, by adopting an internal perspective, the impact of an e-mail is more than the physical impact of electrons. One can point to analogies in physical property that would support treating unwanted e-mail as a trespass or no trespass at all. The real question the degree we wish to delegate to owners or not. There is nothing illogical about deciding to include e-mails with invasions that fall within the exclusion strategy but not other electronic invasions that cause only (humanly imperceptible) physical effects.

One possible solution with precedents in the law of physical – even real – property is to adopt the exclusion approach but with a default implied license to enter until notice is given otherwise. In the world of real property, there are some uses that are so widespread and valuable in certain areas that the presumption that they are trespasses if engaged in is reversed. In many areas of the country, there has long been a custom that one could hunt on uncultivated land unless it were posted with no hunting signs.[97] In other words, the law recognized a norm of licenses for hunting, which owners could withdraw if they were sufficiently specific.

Likewise, in some areas cattle are so much more prevalent than crops that the rule is for fencing out rather than fencing in: that is, in those areas, farmers must fence their land in order to be eligible for damages by straying

---

96 Burk, *supra* note 76, at 34. For a criticism of this argument, see David McGowan, this volume.

97 The rule in the United States is that hunters trespass only if the land is under cultivation, is enclosed, or is posted (with a no trespassing sign). McKee v. Gratz, 260 U.S. 127, 136 (1922) (Holmes, J.) ("[There is a] common understanding with regard to the large expanses of unenclosed and uncultivated land in many parts at least of this country. Over these it is customary to wander, shoot and fish at will until the owner sees fit to prohibit it. A license may be implied from the habits of the country."); *see also, e.g.*, Payne v. Gould, 52 A. 421, 421 (Vt. 1902) (noting that Vermont constitution provides that citizens "shall have the liberty in seasonable times to hunt and fowl on the lands they hold, and on other lands not enclosed"); Ellickson, *supra* note 33, at 1383. Pastureland and orchards are usually not considered cropland, but note that in a state such as Florida with important orchard industry, orchards need not be posted. *See* Fla.Stat. § 810.011(6) ("Cultivated land" is that land which has been cleared of its natural vegetation and is presently planted with a crop, orchard, grove, pasture, or trees or is fallow land as part of a crop rotation."); *Cf.* Robert C. Ellickson & Charles Dia. Thorland, *Ancient Land Law: Mesopotamia, Egypt, Israel*, 71 CHI.-KENT L. REV. 321, 342 (1995) (noting in Mesopotamian laws a strict liability for entering cropland and intent-to-steal requirement for trespass in orchards and arguing that this reflects the importance of investment in cropland).

cattle.[98] But the theory here suggests two limits on this principle. First, the choice between fencing in and fencing out is not, as it is sometimes portrayed, a pure cost-benefit test of the type that Coase envisioned for nuisance disputes. The question is not simply whether crops or cattle are more valuable or which is the cheapest cost avoider. To see why not, consider how costly it would be if this cost-benefit test were to occur at the level of individual parcels. If it did, then a drover of cattle would have to do the cost-benefit analysis each time he encountered a new parcel. Instead, what is usually assumed is that the rule will be set for a given district – even though it is not mentioned that individual parcels in that district might benefit from a more fine-grained exception in the other direction. But now consider a district that wants to have a rule of fencing out. This is an exception to the general *ad coelum* rule that people – especially newcomers and third parties – would be familiar with from more general contexts. So, on the information cost theory we should expect some presumption against fencing out that has to be overcome by some significant positive benefits from fencing out over fencing in. We should expect less fencing out than a district-by-district cost-benefit analysis would predict. What little evidence exists on this question suggests that this is so: fencing in, as the pattern consistent with the general *ad coelum* rule is surprisingly prevalent even in areas where cattle-raising is important.[99]

Such solutions, in some sense, have been applied in a more limited way for telephones, where someone is privileged to call but an owner can opt out by signing up for a do-not-call registry (although the exclusion strategy here is not implemented through trespass).[100] Alternatively, one can "fence" one's phone by screening calls and not listing one's number in a directory. In the case of websites and e-mail, one might have a rule that entry is privileged unless the owner "posts" otherwise. And since posting is not difficult for the one doing the posting, the costs of doing this are far less than in the case of hunting.

The one remaining question is the processing costs to users. A notice on a website that entry is conditional on not using the information in certain ways can raise problems. If the warning is not clear, it may overburden users, and the costs would not be internalized to the owner of the website –

---

[98] ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 52-81 (1991).

[99] *See* Merrill & Smith, *supra* note 3, at 388-91. Another aspect of the fencing in versus fencing out choice that is consistent with the information cost theory is that in cases of intentional trespass the rule is fencing in. That is, even in areas in which farmers have to fence out cattle – by exercising their privilege to fence – a cattle driver who intentionally drives his cattle onto unfenced land is nonetheless liable. *Cf.* Light v. United States, 220 U.S. 523, 537 (1911). The exception to the *ad coelum* rule and the farmers' exclusion rights is a narrow one that does not extend to intentional damage. If the exception did extend to intentional harms, the possibilities for strategic behavior would be much increased.

[100] 15 U.S.C. § 7708(a). In additional to the national do-not-call registry, many states have their own similar schemes.

absent legal intervention or at least withdrawal of legal enforcement.[101] Questions of unconscionability would arise, but in a way similar to those involved in mass contracts. Commentators critical of clickwrap licenses need to be more specific about the information problem. A registry (at least for websites) has the virtue of a standardized format that the relevant actors would know about. A registry is property-like in furnishing information to the world at large. Or one might imagine a standardized click-through agreement page that would lower processing costs for viewers, again in a somewhat property-like fashion. The more difficult question is to what extent notice can be furnished individually and idiosyncratically. Nevertheless, general laws enforcing exclusion have more severe notice problems, if individual users may or may not know the law and their interaction with the website does not present the information. For example, if anti-spamming legislation made it illegal to send an e-mail to anyone that turned out not to want it, such a law would lead to severe problems of notice.

Many recent commentators have been very critical of the use of trespass in the digital context. They claim that this reflects a false analogy to property and real property in particular. They further contend that the analogy is an undesirable one because property concepts get in the way of exploiting the non-rival nature of information and the flexibility and interconnectedness of the internet. As with many arguments about the contours of property rights, the foregone benefits of coarse-grained trespass-like rights are more salient than the costs of departing from the basic exclusionary approach. What are the advantages, if any, of the exclusion strategy? Under that approach the delegation to the owner and her sovereignty over the asset allow her to choose among a wide range of uses of the asset without having to justify that use to the outside world.

All this is not to say that the delineation cost advantages of the trespass-like approach outweigh the benefits of more fine-grained regulation. Nor does it mean that the trespass-like approach is as economizing in the context of the Internet as it is in the world of real property. It does suggest that the benefits of exclusion in saving on delineation cost have been underappreciated. And some of the traditional solutions to the foregone benefits of multiple uses – like a default license with the opt-out of "posting" – suggest ways around the major problems that commentators have identified with using the low-cost trespass-like exclusion approach in cyberspace.

B. *Digital Rights Management*

The possibility of digital rights management has also generated a great deal of controversy recently. Opponents claim that actors can achieve

---

[101] For a general theory of legal intervention to keep down the costs of processing legal relations by third parties, see Smith, *supra* note 31.

greater control over content than they could achieve through copyright.[102] One form that digital rights management takes is shrink-wrap licenses, or more recently clickwrap licenses, in which a user is asked to agree to terms before using software. Other forms of digital rights management are built in software that automatically terminates access after a number of uses or after a set period of time. Opponents claim that these actions "propertize" information despite its non-rival nature and should be banned.

Digital rights management is not all that different from self-help measures that owners of ordinary property might take. A prudent owner usually does not rely solely on his right to invoke the law to exclude intruders. Owners use locks and fences to keep intruders out and set conditions on the access of those they let in. But owners' self-help measures do not end there. Owners also sometimes take actions that make the asset less attractive to potential invaders.[103] At first, this might seem paradoxical or problematic, but it should be recalled that fences and locks consume resources too. So it is not so surprising that owners might consume part of an asset in order to protect the (rest of) that asset from invaders.

The sense in which copyright law is like property law is that in both, the right to exclude implicitly vindicates privileges of use. And these privileges in turn include privileges to take actions that make access by others less attractive. Even with respect to information in which no owner has rights, certain actors might be able to use the information while keeping it secret. They can use their other rights – rights to keep intruders off their land and rights to bodily integrity – to protect indirectly the privilege to use the information exclusively.[104] They may supplement these efforts at secrecy with confidentiality agreements.

Thus, in digital rights management, holders of information and those they deal with are bargaining against the backdrop of privileges, some of which are implicitly protected through legal rights to exclude. Even the non-owners – the potential other users of the information – are just exercising their general privileges and contracting over them so that holders of content will not exercise the privilege to exclude. Contracts of this sort are

---

102 *See, e.g.*, Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003); Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. & TECH. 41 (2001); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

103 Douglas W. Allen, *The Rhino's Horn: Incomplete Property Rights and the Optimal Value of an Asset*, 31 J. LEGAL STUD. 339 (2002).

104 Many of the "property rights" of which economists speak are of this character. See John Umbeck, *Might Makes Rights: A Theory of the Formation and Initial Distribution of Property Rights*, 19 ECON. INQUIRY 38, 39 (1981) (giving example of someone who acquires property rights in coconuts because he is the only one who can climb a tree or one who has rights to fish because of special knowledge of where they are located).

no more problematic than other mass contracts.[105] Claims of lack of bargaining power have to be examined carefully, and it is often the case that lack of bargaining power is not well defined. Asymmetric information and the ability to take advantage of unsophisticated customers would be a better justification for intervention than the mere existence of unsophisticated customers.[106] But if a seller faces sophisticated marginal consumers and cannot tell the two types of customers apart, unsophisticated consumers are not readily exploited. These problems are familiar ones. The grounds for regulation are no different from those in other standard form contract settings.

In terms of the strategies for entitlement determination, an often overlooked reason to allow digital rights management is that it does not require any additional definition of entitlements. The holder of valuable information has a certain set of rights and can combine these with an exercise of general privileges (which do not require separate delineation) to achieve protection of valuable information.

The one area of digital rights management that is most amenable to regulation would be schemes that might violate privacy. Those who oppose digital rights management might find an invasion of privacy in software that automatically stops working if the user does not purchase a new code to feed to it, but not all would agree.[107] Certainly, digital self-help by copyright owners and other holders of rights in information threaten privacy more when they send a message to users' computers or even take control of a user's computer. But notice here that the one engaging in self-help has crossed a boundary and, at least under an expansive view that was rejected in *Hamidi*, is committing a trespass.[108] Very little needs to be added to the existing system of entitlements to give users a right not to be subjected to these forms of self-help.

The contracts used in digital rights management and other mass contracts, again, both present third-party information costs, but perhaps to dif-

---

105 David Friedman, *In Defense of Private Orderings: Comments on Julie Cohen's "Copyright and the Jurisprudence of Self-Help"*, 13 BERKELEY TECH. L.J. 1151, 1167-68 (1998).

106 *See, e.g.*, Richard Hynes & Eric A. Posner, *The Law and Economics of Consumer Finance*, 4 AM. L. & ECON. REV. 162, 170-77 (2002); Alan Schwartz & Louis L. Wilde, *Imperfect Information in Markets for Contract Terms: The Examples of Warranties and Security Interests*, 69 VA. L. REV. 1387, 1401-29 (1983); Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic* Analysis, 127 U. PA. L. REV. 630, 646-48 (1979).

107 Compare Cohen, *supra* note 102, at 580-88 (arguing that such DRM threatens privacy); with Friedman, *supra note* 105, at 1164-67 (arguing that this type of DRM does not threaten privacy).

108 Notice that in the criminal context, Orin Kerr describes (and suggests improved interpretations of) a basic structure of access and authorization that corresponds roughly to the exclusion and governance strategies, respectively. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

ferent degrees.[109] Notice of the information-holder's claims and the terms of access are very low cost to furnish but may not be low cost for people to process. But as in the rest of contract law, doctrines like unconscionability can be used to police problems like misleading fine print. And, as long a notice will not be found unless it is effective, furnishers of notice will have some desire to standardize notice. Finally, in competitive markets the incentive to manipulate the process of notice-giving will be constrained somewhat by the bad reputation one would acquire. The contracts and notice-giving that occur in digital rights management might present informational problems but they do not differ in kind from other situations at the property/contract interface and they do not call for solutions that differ in kind from those already familiar from the non-digital world.

C. *Fair Use in Copyright Law*

Opponents of digital rights management often claim that owners' efforts interfere with traditional fair use and that this is a reason to curtail those activities.[110] Part of the disagreement centers around the nature of the entitlement in users under the traditional fair use doctrine. Recently, technological change has driven a wedge between these different conceptions of fair use. In this part, I will argue that fair use is best regarded as a set of privileges defined by carving out exceptions to the rights granted to copyright owners.[111] If so, fair use is like nuisance and many of the other exceptions to exclusion rights in property law in that the exception to the exclusion right allows room for the public's more general privileges to act to come into play. No further specific delineation of these privileges is required.

Different positions on fair use reflect different degrees of withdrawal of owner sovereignty. On the theory sketched above, recent technological

---

[109] *See* Merrill & Smith, *supra* note 55, at 803-08, 825-31 (discussing mass contracting, and some landlord-tenant relations in particular, as presenting information problems at the property/contract interface).

[110] *See, e.g.*, Burk & Cohen, *supra* note 102; Raymond Shih Ray Ku, *Consumers and Creative Destruction: Fair Use Beyond Market Failure*, 18 BERKELEY TECH. L.J. 539 (2003); Samuelson, *supra* note 102. Fair use is codified at 17 U.S.C. § 107. The statute defines fair use in terms of purposes – "purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research" – and calls for evaluation of the use on the basis of mainly use-based factors, which include "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work."

[111] For an insightful application of Hohfeldian analysis and the analysis of different conceptions of fair use as clusters of rights and privileges, see Wendy J. Gordon, *An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 STAN. L. REV. 1343, 1365-78 (1989).

developments point in opposite directions. First, as new ways of communicating emerge, the value of multiple uses of information increases. Normatively, this points in the direction of a wider and more robust public domain, and a torrent of scholarship and advocacy reflects this point of view.[112] At the same time, the multiple and multiplex nature of uses of information and their lack of foreseeability raises the costs of the delineation of legal entitlements. If so, then rights of exclusion protecting implicit privileges of use become more attractive as a way to secure the return on inputs into creation and commercialization of works. Finally, technological change both lowers the costs of contracting and of digital self-help by owners, as discussed earlier, as well as lowering the costs to appropriators of circumventing barriers to information. For more fine-grained legal intervention in this area to make sense, the stakes have to be high enough to make fine-grained delineation of use-privileges or use-rights worthwhile, and off-the-rack rules have to be superior to private efforts at contracting and self-help. This is likely to be a narrow window of situations, although wider than that in patent law.[113]

At the very least, the costs of delineating rights should make us more receptive to owner contracting and self-help and less receptive to special pleas for extraordinary super property rights, including both super robust notions of the public domain and elaborate private anti-circumvention rights. To what extent these measures are warranted exceeds the scope of this Article, but the present framework does highlight an often overlooked cost of such legislation. The more such legislation casts complicated duties on the world, the more we have to worry about whether the information costs they impose on these third parties is worthwhile.[114] This raises information costs if a non-specialist can wind up violating the prohibition and would have a lot of inquiry to do. Particularly if merely speaking about anti-circumvention devices is criminalized, it is doubtful that such duties are consistent with the level of cost one would want in a system of *in rem* rights.[115] At the least, criminal provisions against circumvention need to have stiff *scienter* requirements in order to help steer clear of these problems. In general, specially tailored rights against circumvention and circumvention-related activity partake more of high-information-cost tort law than traditional protections for the right to exclude.

Traditionally, fair use was like nuisance law in that it made exceptions to the basic right of an owner to exclude. Non-owners could avail themselves of the resource through exercise of their general privileges to act because there was not much that an owner without a legal right could do to

---

112 *See, e.g., supra* note 75.

113 *See* Smith, *supra* note 68.

114 *See* Smith, *supra* note 31.

115 The anti-circumvention provisions of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 (2000), are complex and include criminal liability.

prevent the use. In terms of property rules, this was like the Rule 3 situation in which the would-be user (polluter in the nuisance context, fair use user in the copyright context) had the "entitlement" to the resource. But the "entitlement" is a privilege resulting from an exception to a right to exclude in the other party, not a free standing right. If so, then actions by the owner (the resident or the copyright holder) to prevent the use are also fair game; they merely interfere with a privilege not a right.

The would-be user could have a right along the lines of easements and covenants in real property. But in both these latter contexts, rights have traditionally come about through a negotiation resulting in a special right to engage in the use, not as an off-the-rack legal right. The law could employ off-the-rack rights of fair use, but it would involve more costly delineation.

In a sense, both advocates of the public domain and proponents of strengthened copyright are arguing from a shift from fair use as a privilege to some form of off-the-rack claim-right. The proponents of robust fair use would like to replace the fair use privilege with a right to use under which content owners would be under some kind of corresponding duty. This could be a duty to refrain from actions that defeat fair use or it could even be an affirmative duty to promote fair use. The latter would be the most costly to delineate and enforce. As mentioned earlier, affirmative duties in property law are few and far between, and this helps minimize the cost of delineating, enforcing, and obeying the law's duties. Likewise, the extra mandatory protections that content owners would like go beyond traditional exclusion rights in copyright law. Instead of setting up a low-cost signal for a metaphorical boundary crossing, such schemes set up free standing rights that regulate activity at large.

VI. CONCLUSION

Except in the state of nature, entitlements to self-help require some delineation. Strategies for delineating differ in terms of how closely the signals they rely upon are tied to any particular uses of the resources in question. Where these signals are very loosely tied to use, we have something closer to an exclusion strategy in which a right to exclude implicitly protects the owner's interests and privileges in a wide but unspecified group of uses. Such rules tend to be over-inclusive and, if transaction costs prevent further contracting for access by others, can lead to less use than would be ideal. In order to capture the benefits of multiple uses, further delineation employing signals more directly tied to use will be necessary but will also be more costly. To the extent that such a governance strategy is pursued it should be done at least cost. Normatively, off-the-rack governance rules are only warranted when they both are worth the extra cost of delineation and private governance schemes would not be more cost-effective.

Self-help interacts with the scheme of entitlement determination in several ways. What is called self-help can be either a right or a privilege

and can be a by-product of an entitlement structure or specifically regulated. In terms of the framework presented here, privileges of self-help – like a wide range of other privileges – can be implicitly supported by the broad but indirect rights of exclusion. Where stakes are higher, self-help can be provided for as an exception to rights of exclusion, as illustrated clearly in the law of necessity. Only in the most high-stakes situations that involve high transaction costs should the law move towards free standing rights of self-help. The law of self-help, like the law of entitlements more generally, does not show the type of symmetry one would expect on the hyperrealist view that resource conflicts are free standing and that officials are called upon to engage in balancing in an unconstrained fine-grained way. For the same reason that governance looks more attractive on paper than in reality, the more costly ways of providing for self-help look deceptively attractive.

The law's approach to self-help is part and parcel of the general scheme for delineating entitlements and so is subject to the same considerations of cost and benefit. This goes a long way towards explaining the content and contours of self-help in cyberspace. From controversies over trespass to websites, digital rights management, and copyright fair use, the hostility to property analogies stems from the same sources as the advocacy of off-the-rack governance regimes in the legal literature on tangible property. The correct balance between different strategies for delineating legal entitlements – including entitlements to engage in self-help – is ultimately an empirical question. But in the inevitable guess work involved in striking the right balance, the costs of delineating entitlements suggest a light hand in devising detailed regimes to protect owners and non-owner users.

THE TRESPASS TROUBLE AND THE METAPHOR MUDDLE

David McGowan[*]

This article argues that a claim often advanced in the debate over Internet regulation is unsound. The claim asserts that metaphors such as "space" or "place" or "property" cause judges to think of the Internet as similar to physical property, in which persons may stake private claims the law protects from encroachment.[1] Most metaphor claimants contend that cases extending the trespass to chattels tort to Internet disputes show that the claim is true.[2] I therefore use that line of cases to test the claim.

The metaphor claim may be divided into two parts. The first part maintains that property metaphors lead judges to ignore material differences between tangible property and the Internet. The second part maintains that such metaphors constrain judicial thinking and cause judges reflexively to apply physical-world property rules to cases about things like sending e-mail or retrieving price data from an auction site.

The two parts of the metaphor claim are closely related. Judges who discuss differences between conduct related to the Internet and conduct in physical space are less likely to be confused or blinkered by metaphors than judges who do not discuss such differences. The claims are analytically distinct, however.

The first part of the claim can be falsified by checking the opinions to see whether judges discuss the relevant differences between the physical world and the Internet. Judges who discuss the differences at least have not

---

[*] Professor of Law, University of Minnesota Law School. My thanks to Dan Burk, Dan Farber, Eric Goldman, Dan Hunter, Mark Lemley, Mike Madison, Larry Solum, and participants at the George Mason Journal of Law Economics and Policy symposium and the University of San Diego colloquium for their comments. Remaining mistakes are my fault.

[1] Significant arguments advancing at least some version of the claim include Dan Hunter, *Cyberspace As Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 443 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 527 (2003); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 435 (2003); Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 245 (2003); Alfred C. Yen, *Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1211 (2002).

[2] Hunter, *supra* note 1, at 245; Lemley, *supra* note 1, at 527-28. The most significant critique of the tort in this context is Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 48-49 (2000). I defend this extension on utilitarian grounds in David McGowan, *Website Access: The Case for Consent*, 35 LOY. U. CHI. L.J. 341 (2003). For similar criticism, *see Richard A. Epstein, Cybertrespass*, 70 U. CHI. L. REV. 73 (2003).

ignored them, though they might still be confused or constrained. I refer to this part of the claim as the "empirical assertion" of the claim.

The second part of the claim is not strictly falsifiable. Insofar as it can be tested at all, it infers what a judge thought from what she said.[3] The inference could be weak or strong, plausible or implausible, but it cannot be tested as reliably as the claim that an issue was or was not discussed. A confused judge, or one who thought the Internet could be sliced up like real property, might not use the relevant words. A free-thinking, clear-headed judge might use them.[4] I refer to this part of the claim as the "linguistic inference" of the claim.

I offer four reasons to reject the metaphor claim. First, at least with respect to the trespass cases, the empirical assertion of the claim is false. The opinions cited to support the claim discuss the relevant material differences between the Internet and the physical world. The logic of the opinions demonstrates that judges have taken those differences into account in deciding cases.

Second, the linguistic inference of the claim is weak. Because the empirical assertion of the claim is false, the linguistic inference of the claim contradicts itself. It has to assert that judges mean what they say when they use property-like words but not when they discuss the differences between the physical world and the Internet. Moreover, judges have given reasons for extending the trespass tort to Internet cases. Whether judges are confused or have ignored alternative paths depends in large part on whether their reasons are any good. Metaphor claimants have not acknowledged the most significant doctrinal reason courts have advanced for extending the trespass tort. Nor have claimants advanced telling utilitarian arguments against these decisions, and their own utilitarian predictions have been falsified by experience.

Third, for these reasons the metaphor claim is unfair to the judges at whom it is leveled. Though I am sure metaphor claimants do not intend this result, the claim acts as a highly effective rhetorical device that trivializes judicial opinions without engaging them, producing an unenlightening debate in which people talk past each other and take positions as much as they make arguments.

Fourth, analysis of the logical structure of the metaphor claim supports the conjecture that it is the metaphor claimants who are preoccupied with physical-world concepts of property, not the courts. The claim presumes that "property rules" have some unique or intrinsic relation to tangible things like dirt or disk space. Academic analysis of property abandoned this notion long ago. For many years, the dominant use of the term "property" has referred to how people must deal with each other relative to some resource rather than to the resource itself. Judges who use the term prop-

---

[3] Hunter, *supra* note 1, at 469-70.

[4] I address this point *infra* Part IA and as appropriate in the balance of the discussion.

erty therefore do not show themselves to be preoccupied with things, or captive to the thing-ness of physical property.

Part I describes the metaphor claim and shows that courts are not guilty of what the claim charges against them. Part II analyzes the rhetorical structure and function of the claim. Part III explains why advocates of the claim are more bound to traditional conceptions of property than are the judges they criticize.

I

In this Part, I specify what the metaphor claim is and argue that courts are not guilty of doing what the claim claims they are doing.

A. *Scholarly Endorsement of the Metaphor Claim*

One version of the metaphor claim, advanced by Professor Dan Hunter, is that "[t]hinking of cyberspace as a place has led judges, legislators, and legal scholars to apply physical assumptions about property in this new, abstract space."[5] In fact, "[t]he cyberspace as place metaphor leads to a series of metaphorical *entailments*: cyberspace is like the physical world and can be zoned, trespassed upon, interfered with, and divided up into a series of small landholdings that are just like property holdings in the physical world."[6]

Professor Hunter's argument is cognitive. He believes all persons (and therefore all judges) think with and through metaphors, which "structure and mold" their thinking. Decisions are entailed by the metaphors judges employ in thinking about a case.[7] Metaphors may influence thinking at a sub-conscious level, so even judges constrained by metaphors might not recognize the constraint.[8] Language in opinions may evidence the metaphorical constraint, but the constraint would operate even if the language gave no evidence of that fact.[9] Linguistic evidence may be weak or strong, however and, in Part IB, I test such evidence when evaluating the linguistic inference of the metaphor claim. I pause here to note some difficulties with the cognitive approach, which are better discussed at a logical level than in connection with the cases.

Because metaphors may operate subconsciously, and because judicial language may be unreliable or inconclusive evidence of judicial thinking,

---

5 Hunter, *supra* note 1, at 443

6 *Id.* at 472 (emphasis added).

7 *Id.* at 514.

8 *Id.* at 475.

9 *Id.* at 469-71.

the purely cognitive aspect of Professor Hunter's claim is hard to test. Part of the claim could be tested by asking whether a decision could be explained by arguments that do not use place metaphors as a premise.[10] That point does not prove the negative, of course. A judge *might* be constrained by the place metaphor without knowing it, or giving evidence of it in an opinion, even if a different path of reasoning could explain the result. Alternative explanations can weaken the claim that the place metaphor entails certain results, but they cannot refute it.

Professor Hunter's normative argument refutes the strongest reading of his cognitive thesis, however. He opposes what he calls the "cyberspace enclosure movement," a term that refers to decisions and statutes that give website or network owners the right to prevent others from sending queries to (or messages through) a site or network.[11] He also claims the metaphor and its entailments are the "fundamental cause of the cyberspace enclosure movement."[12] At the same time, however, he says the place metaphor affects him as well as everyone else,[13] implying that he is constrained by the entailments of the metaphor, too.[14] This claim tends to blunt an obvious objection to the entailment thesis—that by careful analysis judges might escape their metaphorical bonds—by showing that even those keenly aware of the metaphor cannot escape its force. If that is true, however--if property metaphors cause analysts to favor enclosure in the same way an earthquake causes a freeway to collapse--then a person influenced by the metaphor, as Professor Hunter says he is, will necessarily favor cyberspace enclosure, which Professor Hunter does not.[15]

This analysis shows that the strongest reading of the cognitive aspect of the metaphor claim is refuted by the normative case the claim is supposed to support. It follows that a person may think of cyberspace as place but hold any of a number of different opinions regarding cyberspace "enclosure." Common sense supports that view. Even if we think using place metaphors, it does not follow that we think in no other way, or that, even if we do think only in metaphors, the place metaphor dominates all others. That leaves only the suggestive hypothesis that the metaphor nudges judges (perhaps shoves them) toward enclosure. Unfortunately, except to the extent it can be tested by the language and logic of opinions, that hypothesis is indistinguishable from the assertion that, because courts disagree with me, ergo they are confused, constrained, or just do not get it. *That* assertion is a condescending *non sequitur.*

---

[10] In Part IB, I suggest the trespass cases can be explained by cost-benefit analysis. If one had to pick a metaphor for such analysis, competition (games) would be a more likely metaphor than "place."

[11] *Id.* at 514.

[12] *Id.* at 514.

[13] *Id.* at 446.

[14] *Id.* at 472.

[15] *Id.* at 503.

Other scholars advance versions of the metaphor claim that are more linguistic and less deterministic than Professor Hunter's cognitive view. Professor Michael Madison suggests that "[p]lace metaphors rule. Trespass . . . cases so far suggest that courts have failed to appreciate the depth and complexity of the Internet- as-place metaphor, particularly in light of how users actually experience places on the Internet."[16] Thus, "courts have erred by relying on an Internet-as-place metaphor without properly connecting that metaphor to interests in intangible information that have been at issue."[17] Commenting on Professor Hunter's article, and referring to "courts misled by metaphor," Professor Mark Lemley agrees that "several courts have made the mistake of overlooking the differences between the Internet and physical space in a variety of contexts,"[18] though he believes courts "could get the cases right—even within the framework of the cyberspatial metaphor."[19]

As this brief survey suggests, different scholars have different opinions regarding how important property metaphors are. Professor Hunter sees them as being crucial—entailing decisions and constraining results—while Professors Madison and Lemley think metaphors are significant but not decisive. Each of these scholars worries, however, that, either consciously or subconsciously, metaphors will cause or tempt judges to think something like: "cyberspace is a place; places are comprised of property; property is property is property; we know what rules govern property; ergo we know what rules should govern the Internet; let's go home."

B. *The Metaphor Claim Does Not Describe Fully the Opinions It Criticizes, and It Supports Only A Weak Inference of Judicial Confusion*

Are judges really constrained or misled by metaphors? To the extent one can answer this question at all, and to the extent one can do so from the trespass cases, the answer is no. In this section I show that judges have not overlooked what scholars see as important distinctions between cyberspace and the physical world, so the empirical assertion of the claim is false. I also show that the reasons judges have given for their decisions form valid arguments and are inconsistent with the idea that judges are confused, so the linguistic inference of the claim is weak.

This section tests the metaphor claim by examining cases extending the trespass to chattels tort to the Internet context. Professors Hunter,[20]

---

16 Madison, *supra* note 1, at 436.

17 *Id.* at 485.

18 Lemley, *supra* note 1, at 527.

19 *Id.* at 530.

20 Hunter, *supra* note 1, at 485-86.

Madison,[21] and Lemley[22] all point to such cases as evidence that the claim is true. The connection between the metaphor claim and the trespass tort rests on an influential article by Professor Dan Burk.[23] For this reason, I discuss his work as well, though he does not advance the metaphor claim as such.

I will begin by describing the black-letter of the tort before courts started using it in Internet cases. Section 217 of the *Restatement (Second) of Torts* defines the tort of trespass to chattels as the intentional dispossession of a chattel belonging to another, or the use of or intermeddling with a chattel in the possession of another.[24] Section 218 of the *Restatement* recognizes a cause of action for dispossession or intermeddling that harms the chattel or an owner's chattel-related legal interests. Harmless intermeddling with a chattel is a trespass, but it does not support a cause of action against the trespasser.[25]

In this respect, the tort of trespass to chattels differs from the tort of trespass to land, where a cause of action lies even if the defendant's trespass causes no harm. The difference is in the cause of action, however, not in the legal interests the two torts recognize. Comment e to *Restatement* Section 218 makes this point clear. Several of the opinions at which the metaphor claim is leveled quote this comment in full, so I will do so here. I italicize the last sentence because the most important opinion extending the tort did so, and because that sentence is commonly omitted in criticisms of that extension:

> 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. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, 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, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c). *Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.*[26]

Thrifty-Tel, Inc. v. Bezenek[27] set the stage for judges to extend the trespass tort to the Internet. Metaphor claimants do not cite it, but courts do, and the metaphor claim rests in part on a criticism of it, so I mention it

---

21 Madison, *supra* note 1, at 467-68.

22 Lemley, *supra* note 1, at 527-28.

23 Burk, *supra* note 2.

24 RESTATEMENT (SECOND) OF TORTS § 217 (1965). Comment e to Section 217 defines "intermeddling" as "intentionally bringing about a physical contact with the chattel."

25 RESTATEMENT (SECOND) OF TORTS § 218 (1965).

26 RESTATEMENT (SECOND) OF TORTS §218 cmt. e (1965).

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

briefly here. The case involved a claim for conversion of access codes to a telephone system. The plaintiffs won at trial, but the appellate court thought the conversion tort did not extend to intangibles,[28] such as access codes (the acquisition and use of which does not deprive the owner of them), thus demonstrating that the court knew it was dealing with intangibles. If the empirical assertion of the metaphor claim were applied to this case, this discussion would refute the assertion.

The court used the trespass to chattels theory to get around the problem that the conversion tort does not extend to things that can be taken without taking them away from the owner. If the linguistic inference of the claim were applied to this case, the court's reasoning would provide little basis for it. The court did draw an analogy to cases where a plaintiff alleged trespass when dust or other particulates fell on property (real and personal), but it acknowledged that the cases were analogous, not identical.[29] The conduct at issue in *Thrifty-Tel* had caused network congestion,[30] so the analogy was defensible, though not irresistible.

Thrifty-Tel is also significant because Professor Burk accused the court of confusing land and chattel. He said the court "blithely glosse[d] over" the difference between land and chattel, "noting simply that both legal theories share a common ancestry."[31] To the contrary, the court discussed the evolution of the tort and said it survived as a "little brother of conversion," which is how the court used the tort.[32] This charge of confusion ripples through the metaphor claim, but the opinion does not support it.

Citing *Thrifty-Tel*, *CompuServe, Inc. v. Cyber Promotions, Inc.*,[33] applied the trespass tort to the Internet and extended the cause of action to a case where the defendant's conduct did not harm hardware or congest bandwidth. Cyber Promotions sent unsolicited bulk e-mail (spam) to CompuServe customers, who complained to CompuServe.[34] CompuServe demanded that Cyber Promotions stop, and tried to block the spam. Neither strategy worked,[35] so CompuServe sued.

---

28 *Id.* at 472.

29 *Id.* at 473 n.6 (collecting cases).

30 *Id.* at 471.

31 Burk, *supra* note 2, at 33. Professor Burk's article also said "the `particulate trespass' cases" the court cited "were largely cases in which the owner of real property had been dispossessed of the use of the land by contamination." *Id.* at 33-34. That description of the cases is not accurate. The *Thrifty-Tel* court cited four particulate trespass cases. Each did indeed involve land. None of the plaintiffs were put off their land, however—all the plaintiffs lived on their land—and no case mentioned ways in which the plaintiffs were prevented from using their land. Professor Burk informs me the unusual "dispossessed of use" language is attributable to a student error in the editing process.

32 54 Cal. Rptr. 2d 468, at 472-73.

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

34 *Id.* at 1019.

35 *Id.* at 1019, 1023.

Like the court in *Thrifty-Tel*, the *CompuServe* court considered the conversion tort but then enjoined the spam on the trespass theory.[36] The opinion in *CompuServe* therefore refutes the empirical assertion of the metaphor claim. The court not only did not ignore the difference between physical property and intangibles, it cited that difference in deciding to rely on the trespass theory rather than the conversion theory.

Some language in *CompuServe* tends to support the linguistic inference of the metaphor claim. The court said CompuServe had "a possessory interest in its computer systems" and that Cyber Promotions' spamming amounted to intentional contact (via electronic charges) with those systems.[37] It also said Cyber Promotions' messages "demand the disk space and drain the processing power of plaintiff's computer equipment," so "those resources are not available to serve CompuServe subscribers."[38] In justifying its injunction, it said "the public interest is advanced by the Court's protection of the common law rights of individuals and entities to their personal property."[39]

Other language in the opinion undercuts the linguistic inference, however, and this undercutting language is tied more directly to the holding than the language I just quoted. The opinion discussed Cyber Promotions' use of hardware not because it thought physical property and bandwidth are identical, but to establish a doctrinal hook necessary to address what the court saw as the real economic issue in the case. The court stressed that Cyber Promotions' spam harmed CompuServe's business. It emphasized that CompuServe customers wasted time (and therefore money) deleting Cyber Promotions' spam; many customers complained, and some quit the service.[40] Later in the opinion, in connection with a First Amendment claim, the court indicated it was concerned that CompuServe and its customers not bear the marginal cost of running Cyber Promotions' business.[41] This discussion takes into account all the social costs of Cyber Promotions' business, which an approach that considered only harm to hardware would not do. The court's approach reflected good utilitarian analysis, not confusion.

The *CompuServe* court's doctrinal analysis of the trespass tort undermines the linguistic inference even more than the court's economic analysis. The court recognized that, under the Restatement, harm is an element of the trespass to chattels tort but not of a claim for trespass to land. Rather than simply noting this fact and stopping, however, the court analyzed the

---

36 *Id.* at 1022 ("A plaintiff can sustain an action for trespass to chattels, as opposed to an action for conversion, without showing a substantial interference with its right to possession of that chattel.").

37 *Id.* at 1021.

38 *Id.* at 1022.

39 *Id.* at 1028.

40 *Id.* at 1019, 1023.

41 *Id.* at 1026.

purpose behind each set of elements. It concluded that there is a "*reason* that the tort of trespass to chattels requires some actual damage as a *prima facie* element, whereas damage is assumed where there is a trespass to real property."[42]

The court found the reason for this difference in the comment to Section 218. The court block-quoted the language of that comment, as I did a moment ago,[43] and it italicized the same language: "*Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.*"[44] The court concluded that CompuServe had a trespass claim because it suffered economic harm to its business (though not to its system) and because its self-help efforts had not worked. Because the self-help the *Restatement* expected to be "sufficient" to protect CompuServe's interests had failed, the court protected that interest by extending the cause of action to compensate for the failure.[45]

The court's default rule of access also is inconsistent with the linguistic inference. The court recognized that "[a] great portion of the utility of CompuServe's e-mail service is that it allows subscribers to receive messages from individuals and entities located anywhere on the Internet," so it held that "there is at least a tacit invitation for anyone on the Internet to utilize plaintiff's computer equipment to send e-mail to its subscribers."[46] Trespass claims would lie only if defendants persisted in use after notice of the plaintiff's objection.[47] To the extent property metaphors imply a "default rule of exclusion,"[48] the court's default rule of permission is inconsistent with the claim that property metaphors controlled the case.

Combined with the court's discussion of harm to CompuServe's business, these passages rebut the linguistic inference as much as anything can. The court did not think the important issue in the case concerned CompuServe's hardware; the discussion of customer losses and free riding contradicts that idea. Nor did it think chattel could be treated reflexively as real property; its careful analysis of the differences in the two torts and its concern for the failure of CompuServe's self-help privilege contradict that idea. Even for those who believe metaphors are inescapable, the court's marginal cost analysis suggests competition—the metaphor of a game or a race—explains the opinion at least as well as the metaphor of place.

---

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

43 *See supra* text accompanying note 26.

44 *CompuServe*, 962 F. Supp. at 1023; RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965).

45 Indeed, the court implied that the failure of self-help had to be alleged to state a claim for harmless intermeddling. 962 F. Supp. at 1023.

46 *Id.* at 1023-24.

47 *Id.* at 1024.

48 Hunter, *supra* note 1, at 507-08. Professor Hunter notes that his characterization of a default rule of exclusion may not be strictly accurate, so the inconsistency in the text is simply an inconsistency, not a contradiction.

eBay, Inc. v. Bidder's Edge, Inc.,[49] extended the trespass tort to a situation involving neither harm to hardware nor proven economic loss to the plaintiff's business. eBay hosts Internet auctions.[50] Using automated browsing programs (robots), Bidder's Edge collected auction prices from different sites and displayed them on its own site, providing one-stop comparison shopping among auctions. It did not host auctions itself, so its business model focused only on buyers, not sellers.[51] Because eBay was the largest auction site, Bidder's Edge needed prices from eBay auctions.[52] At first eBay and Bidder's Edge agreed on terms on which Bidder's Edge could get the price data. They later disagreed, however, and eBay demanded that Bidder's Edge stop using robots to query eBay's site.[53] Bidder's Edge continued to do so; eBay tried to block its automated queries, the self-help failed, and eBay sued.[54]

The court's opinion refutes the empirical assertion of the metaphor claim. The court discussed the difference between a claim for conversion and a claim for trespass,[55] and adopted the trespass theory because Bidder's Edge's intangible queries would not support a conversion claim.[56] Though the court twice mentioned physical spaces, each reference distinguished such spaces from eBay's site.[57] In light of such explicit analysis, the *eBay* court cannot fairly be said to "have had land rather than information in mind" when it ruled.[58]

Some of the court's language could be read to support the linguistic inference of the metaphor claim. The court said eBay had a "possessory interest in"[59] and a "fundamental property right to exclude others from" its system.[60] It said eBay's servers were "private property,"[61] and it agreed with

---

49 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

50 *Id.* at 1060.

51 *Id.* at 1061. For this reason, it is only partly accurate to describe Bidder's Edge as a competitor of eBay. *Cf.* Hunter, *supra* note 1, at 484 n.292. I discuss this point further *infra* Part IIB.

52 *eBay*, 100 F. Supp. 2d at 1062. Sixty-nine percent of the auction items listed on Bidder's Edge were from eBay auctions. *Id.* at 1063.

53 *Id.* at 1062.

54 *Id.* at 1062-63; *see also* McGowan, *supra* note 2, at 350.

55 *eBay*, 100 F. Supp. 2d. at 1067.

56 *Id.*

57 *Id.* at 1067 (auction house). *Id.* at 1065-66 (store). For example, the court said a physical-world auction house could reserve seats only for actual bidders, but that this fact meant little in the case because Bidder's Edge's queries did not displace actual bidders. *Id.* at 1067. This comment refutes the idea that the court did not understand "that the requests for information that . . . Bidder's Edge sent did not exclude others from using the site." Lemley, *supra* note 1, at 528. Professor Hunter correctly notes that the court rejected this analogy to physical space, but he believes the "cyberspace as place metaphor was operating here, even though the court did not ultimately accept eBay's argument." Hunter, *supra* note 1, at 484.

58 Lemley, *supra* note 1, at 529.

59 *eBay*, 100 F. Supp. 2d at 1070.

60 *Id.* at 1067.

eBay that Bidder's Edge's queries appropriated "eBay's personal property by using valuable bandwidth and capacity . . . compromising eBay's ability to use that capacity for its own purposes."[62] The court was concerned that, even though Bidder's Edge's queries used "only a small amount of eBay's computer system capacity," Bidder's Edge "nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes."[63] It held that "[t]he law recognizes no such right to use another's personal property."[64] The court also worried that a ruling for Bidder's Edge might "encourage frequent and unregulated crawling to the point that eBay's system will be irreparably harmed."[65] On the facts of the case, however, this comment was unpersuasive if not wholly fanciful speculation.

There are three reasons why this language does not support a strong inference of linguistic confusion, and why the opinion as a whole supports only a weak inference, if any at all. First, as in *CompuServe,* the *eBay* court's rejection of the conversion tort cuts against the inference because it shows the court knew it was dealing with intangible "information" in the form of queries to a server and the server's responses. Second, the *eBay* court was aware of and discussed the difference between the torts of trespass to chattels and trespass to land.[66] Like the court in *CompuServe* (which it cited on this point), the court block-quoted comment e to Restatement Section 218, including the comment's language regarding self-help.[67] The court had noted that eBay's self-help efforts to block Bidder's Edge's queries had failed,[68] though it did not repeat that fact after quoting the Restatement.

Third, and most telling, the court discussed the case as a problem of contracting. It noted that (i) the parties originally had an agreement allowing Bidder's Edge to browse;[69] (ii) negotiations toward a new agreement broke down;[70] and (iii) according to Bidder's Edge, eBay had "engaged in a pattern of licensing aggregators to crawl its site."[71] The court said eBay's

---

61 *Id.* at 1070.

62 *Id.* at 1071.

63 *Id.*

64 *Id.*

65 *Id.* at 1067.

66 Citing *CompuServe,* the court noted that harm is an element of a cause of action for intermeddling with chattel. It then said "[t]he Restatement offers the following explanation for the harm requirement," and quoted comment e to Section 218. *Id.* at 1071.

67 *Id., quoting* RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965).

68 *eBay,* 100 F. Supp. 2d at 1062-63.

69 *Id.* at 1061.

70 *Id.*

71 *Id.* at 1067. That allegation—which came from Bidder's Edge—suggests eBay's refusal was not an attempt to use market power to crush a competitor. *Cf.* Hunter, *supra* note 1, at 484 n.292. If that were eBay's game, why would it license any aggregator at all? The Antitrust Division of the Justice Department investigated eBay's licensing practices, but took no action against it. Ira Steiner, *Justice Department Closes Antitrust Investigation Against eBay, Company Reports,* AUCTION BYTES March 26,

suit "appears to be, in part, a tactical effort to increase the strength of its license negotiating position and not just a genuine effort to prevent irreparable harm."[72] And it said that "[i]f preliminary injunctive relief against an ongoing trespass to chattels were unavailable, a trespasser could take a compulsory license to use another's personal property for as long as the trespasser could perpetuate the litigation."[73] It was right about that.

Though the court did not cite the economic literature regarding the difference between injunctions and property rules, on the one hand, and damages and liability rules, on the other,[74] the opinion may fairly be read as clarifying eBay's legal interest by extending the trespass cause of action so eBay could force Bidder's Edge to internalize the cost eBay believed Bidder's Edge imposed on eBay and its sellers. That choice does not reflect confusion between the physical world and the Internet, or between disk space and data. It is in fact a fairly sophisticated form of transaction-cost economic analysis.[75]

Register. com, Inc. v. Verio, Inc.,[76] also sheds light on the contractual aspect of such cases. Register.com, the plaintiff, registered Internet domain names and provided related services to its clients. Its registration agreements allowed clients to "opt in" to receive solicitations from Register.com or firms with which it contracted.[77] The agreement that authorized Register.com to register domain names required it to maintain list of contact information for the sites it registered.[78] Verio competed with Register.com in providing services to firms that registered domains, but Verio was not a registrar itself. Using a robot, Verio browsed Register.com's list of clients each day, and then sent those clients unsolicited e-mail pitching Verio's services.[79] At first, these e-mails mentioned that the recipient had recently registered a domain with Register.com, so some customers thought Register.com was spamming them, contrary to its opt-in policy. Some customers complained to Register.com about these e-mails.

2002 (available at http://www.auctionbytes.com/cab/abn/y02/m03/i26/s02) (last visited March 8, 2004). Some auction aggregators remain in businesss. www.auctionbeagle.com (last visited March 25, 2004).

72 *Id.* at 1064.

73 *Id.* at 1067.

74 For a review of this literature in the present context, see McGowan, *supra* note 2, at 342-43, 375-76.

75 *Id.* at 375-76. For this reason, if one insists that metaphors are inescapable modes of thought, the game metaphor explains these aspects of the opinion at least as well if not better than the place metaphor. The two might be hard to distinguish, for reasons I discuss in Part III.

76 356 F.3d 393 (2d Cir. 1994).

77 Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 241 (S.D.N.Y. 2000), *aff'd* 356 F.3d 393.

78 This agreement was between Register.com and the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit corporation established by the U.S. government to operate the Internet domain name system. 356 F.3d at 395.

79 *Id.* at 396-97.

Contrary to the contract under which it was authorized to register domain names, Register.com tried to place conditions on the use of its customer list. Responses to queries to that list included a legend stating that, by querying Register.com's list, the recipient agreed not to use the list to spam the listed customers.[80] When it found out what Verio was doing, Register.com demanded that Verio stop. It claimed Verio was harming its business and violating the conditions it placed on use of its customer list. The district court enjoined Verio, in part on a trespass to chattels theory, and the Second Circuit affirmed.

Register.com did not break new ground on the trespass tort.[81] It is interesting, however, because of its approach to the question of how courts should treat form conditions on the use of posted data. Verio claimed it was not bound by Register.com's conditions because those conditions were only contained in replies it received *after* its robots queried Register.com's computers.[82] The Second Circuit said this argument might be persuasive if Verio had submitted only one query, or a few sporadic queries, but it rejected the argument in the case at hand because Verio queried Register.com's customer list many times each day. It got the list of conditions in response to every query, and it admitted that it "knew perfectly well what terms Register demanded."[83]

At a minimum, *Register.com* holds that a site user is bound by conditions a site owner places on the use of posted data when the user has actual notice of those conditions before submitting queries to the site.[84] Because the plaintiff's notices were contained in replies to Verio's requests, the court did not address the question whether a user would be bound by terms that were posted on a site, conspicuously or otherwise. The *means* of giving notice is still an open question. Site owners are unlikely to sue without providing actual notice in the form of a demand that a user change its ways, however, so this question may be of little practical significance.

---

80 *Id.* at 396.

81 The court of appeals only affirmed the district court's highly speculative finding that, if Verio's unauthorized querying were allowed, then other firms would submit such queries, too, and Register's system would crash. *Id.* at 404. As with *eBay*, there is no reason to believe this risk is substantial. Both findings are better read as predicates necessary to support a property rule than as accurate descriptions of real-world probabilities. I sympathize with those frustrated by such pretextual findings.

82 *Id.* at 401.

83 *Id.* It was on this basis that the court distinguished *Register.com* from Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002), which refused to enforce a term the defendant could have seen by scrolling down a page but which the defendant did not see on his one visit to the site. 356 F.3d at 402.

84 The court rightly said "[i]t is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree." 356 F.3d at 403.

Contract issues relate to the trespass tort in two ways. The first has to do with traditional doctrine. Site owners have a legal interest in the exclusive possession of their systems; users therefore have no legal right to use such systems.[85] Thus, even if traditional doctrine gives site owners no tort cause of action for harmless intermeddling, owners still have something to convey to site users: the legal right to use hardware users otherwise have no right to use. Even under traditional doctrine, therefore, the owner's interest in chattel might be enough to support a contract claim, assuming contractual prerequisites were met. Damages might not be high but, in a case like Verio, specific performance might be ordered on the ground that losses in goodwill are hard to measure.[86]

That argument seems strange, however. Why would a rational site user agree to be bound by an owner's conditions when the owner could not sue the user (at least in tort) so long as the user caused no harm to the owner's system? If no rational user would assent in such a case, it seems odd to say the user has "assented" to the owner's terms by querying the site. That strangeness highlights the fact that legal interests and remedies go together. A right without a remedy is just a suggestion. That is the second point tying trespass and contract together. By making it clear why a user like Bidder's Edge or Verio might agree to a site owner's terms, judicial extension of the trespass tort eliminates the strange fit between contract and a site owner's interest in the exclusive possession and use of its system.

Many scholars decry the use of form contracts to condition access to or use of information.[87] Criticism often claims that form agreements pertaining to software or websites alter traditional contractual principles. *Register.com* correctly rejects that claim.[88] Other objections predict dire results if courts enforce conditions on the use of networks or information. I discuss such claims in Part IIB; the bottom line is that they are not supported by logic or the opinions they criticize. Extension of the trespass tort therefore nicely complements contract decisions such as *Register.com*, which are to be welcomed rather than condemned.

The last case I will discuss is *Intel Corp. v. Hamidi*.[89] Hamidi is a former Intel employee, unhappy with the firm because it fired him. After being fired, Hamidi sent to between 8,000 and 35,000 Intel employees six different e-mails criticizing the firm. Like CompuServe and eBay, Intel asked Hamidi to stop, tried to block his e-mails, and then sued him when neither tactic worked. The trial court ruled for Intel on a trespass to chattels theory, and enjoined Hamidi from sending Intel any more mass e-mails.[90]

---

85 *See supra* text accompanying note 64; *infra* text accompanying note 106.

86 *See* RESTATEMENT (SECOND) CONTRACTS § 359 (1981).

87 For a collection of objections, see Madison, *supra* note 1 at 447-64.

88 356 F.3d at 401.

89 114 Cal. Rptr. 2d 244 (Ct. App. 2001), *rev'd* 30 Cal. 4th 1342 (2003).

90 *Id.* at 246.

The court of appeals affirmed this ruling. The language of the opinion refutes the empirical assertion of the metaphor claim. The court began its analysis by stating that it sought to adapt the trespass to chattels tort to new circumstances.[91] Citing briefs filed by the ACLU and Electronic Frontier Foundation, the court acknowledged the view that "'cyberspace' . . . is necessarily free and open, minimizing the harm caused to Intel's business."[92] It rejected this view, however, because the argument focused only on harm to hardware and ignored harm to the productivity of Intel's workers, and thus to Intel's business, which the court thought should not be ignored.[93] As in *CompuServe,* the court's decision to consider all the costs and benefits of Hamidi's actions reflects sound utilitarian analysis, not confusion.

Similarly, the court acknowledged and rejected the argument that, if Intel won, then all unsolicited e-mail would constitute a trespass. Like the *CompuServe* court before it,[94] the court presumed consent to such communications and held that a cause of action would lie only if a user persisted in some conduct after a site owner notified a user that the owner objected to the use.[95] The court's default rule reflects its understanding that the basic purpose of the Internet is to exchange information, and that denial of permission to do so is the exception rather than the rule.

The intermediate appellate opinion in *Hamidi* provides weak support for the linguistic inference of the metaphor claim. The discussion in the preceding paragraph shows the court knew the harm at stake was harm to Intel's business, not its hardware. As in *CompuServe* and *eBay*, the court quoted the full text of comment e to *Restatement* section 218, which we have examined in enough detail already.[96] The court noted that Hamidi acknowledged Intel's right to try to block his e-mails, and that its self-help efforts had failed. The court thought Hamidi would probably keep trying to defeat Intel's efforts, and it enjoined Hamidi in part to put an end to what it saw as "this wasteful cat-and-mouse game" that produced "no public benefit" sufficient to deny Intel's request for injunctive relief.[97] None of this analysis bespeaks confusion.

Professor Hunter has pointed to one portion of the opinion he believes supports the linguistic inference of metaphor claim.[98] In rejecting Hamidi's First Amendment claim, the court referred to Intel's hardware as its "private property."[99] Professor Hunter believes "[t]he court should have said that Hamidi trespassed against Intel's personal property, or some other language

---

91 *Id.* at 247.

92 *Id.* at 249-50.

93 *Id.*

94 CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1024 (S.D. Ohio 1997).

95 114 Cal. Rptr. 2d at 250.

96 *See supra* text accompanying note 26.

97 144 Cal. Rptr. 2d at 249.

98 Hunter, *supra* note 1, at 487-88.

99 144 Cal. Rptr. 2d at 254.

that indicated that the chattel was misappropriated or abused. Instead, the court clearly had the real-property action in mind when it dismissed the First Amendment claim."[100]

It is reasonable to interpret some of the court's references to "private" property as supporting the linguistic inference of the metaphor claim. I believe Professor Hunter overstates the significance of these references, however. The law contrasts "personal" property with "real" property, a term the court used only once, when it distinguished cases Hamidi cited on the ground that those cases "involved claims of damage to realty, not chattels."[101] The court distinguished defamation cases on the ground that, in *Hamidi*, "the speaker's rights are pitted against a property owner's rights—of at least equal constitutional force—to wisely govern his lands (or, in this case, his chattels)."[102] These passages cut against Professor Hunter's interpretation.

In addition, the court rejected the First Amendment claim on state action grounds.[103] "Private" in this portion of the opinion contrasts with "public," not "personal." The court's point was simply that Intel's servers belong to Intel; they are not like sidewalks or parks. Many of the court's references to "private" property discussed cases that involved realty, and "private property" is a fair term to use to describe these precedents. (In fact, the court's claim that Hamidi trespassed "onto" Intel's property seems to me to provide more support for Professor Hunter's view than the court's use of the word "private.")[104] On balance, the appellate opinion in *Hamidi* cuts against the linguistic inference of the metaphor claim.

The California Supreme Court reversed, and ruled in favor of Hamidi.[105] It correctly noted that the Restatement version of the tort did not provide a cause of action for harmless intermeddling. It held (probably correctly) that under traditional trespass doctrine, only harm to hardware counted; harm to Intel's business did not.[106] The court did not deny that Intel had a legal interest in the inviolable possession of the chattel that made up its network, however, and it did not say Hamidi had a *right* to use Intel's system. It said only that the trespass tort would not defend Intel's interest, creating the extraordinary case of an interest the law recognized but for the infringement of which the law provided no remedy.[107]

---

100 Hunter, *supra* note 1, at 487-88.

101 144 Cal. Rptr. 2d at 251.

102 *Id.* at 253.

103 *Id.*

104 *Id.* at 254.

105 30 Cal. 4th 1432 (2003).

106 *Id.* at 1346. On why the Court's reading was probably correct, *see* Burk, *supra* note 2, at 35.

107 *Id.* at 1357 quoting Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1566 (1996). The court said instead that, "[w]hile one may have no *right* temporarily to use another's personal property, such use is actionable as a trespass only if" the use causes injury to the chattel.

The Court rejected the extension of the tort to provide a cause of action for harmless intermeddling. The court said it was influenced by arguments raised by scholars who warned that affirming the appellate court's ruling would harm the Internet.[108] (We will examine these arguments in Part II.) It also noted contrary arguments raised by Professor Richard Epstein. It decided it would not try to resolve this debate, but it reversed the court of appeals to avoid "acting rashly."[109]

In many contexts, the majority's restraint and deference to legislative expertise would be admirable. In *Hamidi*, however, the appearance of restraint was misleading. The court was not dealing with a situation in which a party asked the court to change an existing doctrine to produce a new and different result the party desired. As every court since *CompuServe* had stressed, self-help did not work in the Internet environment, so in these cases the old doctrine already produced different results than it had in the past. The only question was whether to extend the cause of action to protect the existing interest, or decline to extend the cause of action and leave the interested unprotected. The court chose the latter course, producing a legal result that is highly unusual.[110]

It is therefore no surprise that the Court did not fully acknowledge what it had done. Unlike the opinion it reviewed, the court mentioned the failure of Intel's self-help only in passing,[111] and it did not connect the failure of Intel's self-help remedy to Intel's legal interest in controlling use of its chattel.[112] The court therefore did not confront the appellate court's main argument, the same argument courts had used since *CompuServe,* which was that the doctrine should change to protect the legal interest at stake when the means the old doctrine presumed adequate to protect that interest no longer worked. The *Hamidi* court seemed to believe it could maintain the status quo by declining to extend the tort trespass tort, but it was wrong.

None of these cases supports the empirical assertion of the metaphor claim. Each court focusing on the trespass claim acknowledged differences between the physical world and the Internet, and between tangible and intangible property.[113] Nor does any case support a strong linguistic inference of confusion or blinkered thought. Courts in these cases discuss hardware while deciding on the basis of overall cost-benefit analysis, including harm

---

108 *Id.* at 1347.

109 *Id.* at 1349.

110 McGowan, *supra* note 2, at 359 n.123.

111 The reference takes up one clause of one sentence. 30 Cal. 4th at 1388.

112 *See supra* note 102.

113 I qualify this statement because the *Register.com* court, which upheld a trespass claim but focused more on contract, did not contrast intangible queries with tangible things. The district court's findings of fact show that both it and the court of appeals knew what they were talking about, however. *See* Register.com, 126 F. Supp. 2d at 244-44 (discussing robots and focusing on their queries rather than on hardware); 356 F.3d at 396-97 (same).

to a site owner's business rather than just harm to hardware. That is just sound utilitarianism.

Some valid objections may be raised to opinions extending the trespass tort, but these objections are not telling, and they do not support the metaphor claim very well. One objection is that the *Restatement* does not compel courts to extend the trespass cause of action to compensate for the failure of owner self-help. That is true, but the reasons supporting the extension are sound while the reasons opposing it are weak, a topic I discuss in Part IIB.

Another objection is that courts indulge in fanciful speculation about harm to networks that might occur if everyone in the Internet world suddenly descended on a plaintiff's server, a contingency so far-fetched that its expected cost is trivial. Courts have engaged in such flights of fancy, but that fact signifies little. Such discussions are best read as recitations needed to adapt traditional trespass doctrines to new circumstances, in which self-help fails and owners need some other way of securing the consent that allows them to equilibrate the costs and benefits of resources into which they have sunk costs. Analysis of the economics in these cases, rather than the doctrinal rhetoric, shows that the opinions undercut rather than support the linguistic inference.

II

So what does the metaphor claim do if it does not describe what courts are doing? What is it good for? This Part analyzes the rhetorical effect (not design) of the metaphor claim. It contends that the claim tends to trivialize judicial reasoning without refuting it, while tending to mask weaknesses in the arguments used to criticize the opinions.

I do not believe trespass critics or metaphor claimants intend these effects. I take it for granted that their criticisms are grounded in genuine and deeply held convictions regarding how the law should deal with human behavior on the Internet. Unfortunately, however, the trespass critique is based on a doctrinal error that has rippled through academic criticism and is a significant premise of the metaphor claim.

A. *The Metaphor Claim Trivializes Judicial Reasoning Without Refuting It*

This section argues that the metaphor claim trivializes judicial reasoning without refuting it. Trivialization is to some degree inherent in any claim that a decision-maker has "ignored" facts or been "misled" by words. Decisions by uninformed or confused persons are generally unreliable. If a person is uninformed or confused about the Internet, it is easy to believe they "just don't get it," and there is little point in debating them. By exten-

sion, the views such persons express can be discounted, because persons who do not "get it" are unlikely to say meaningful things about "it" (the "it" in this sentence being "cyberspace").

The metaphor claim trivializes opinions to a very high degree because those who level the claim do not discuss all the reasons judges have given for the decisions they criticize. Except for *Thrifty-Tel,* the opinions discussed in Part 1 block-quoted comment e to Section 218 of the *Restatement,* noted that chattel owners have a legal interest in inviolable possession of chattel as against even harmless intermeddling, and noted that the self-help the *Restatement* said would be "sufficient" to protect this interest had failed in the case at hand. The one case to reject the extension--the California Supreme Court opinion in *Hamidi*—was also the one case not to acknowledge this argument.

I am not aware of any article criticizing the trespass tort or advancing the metaphor claim that discusses this argument, much less refutes it. To the contrary, scholars who assert the metaphor claim sometimes quote the beginning and middle of comment e, which contrasts chattel with land, without quoting the end of the passage, which courts since *CompuServe* have used as the basis for extending the cause of action.[114] In one case, such a partial quotation is used to support the claim that courts have "ignored" the harm requirement of the tort; courts have in fact used the omitted portion of the comment as a reason for modifying that requirement.[115] In another case, a partial quotation of comment e is followed by the statement that the appellate court in *Hamidi* "relie[d] on a theory of 'inviolability' that has never been the rule for personal property."[116] In a third case, that statement precedes the partial quotation.[117]

The "it has never been the case" argument is almost always a weak one. Setting aside the usual problem of deriving ought from is,[118] and

---

114 Hunter, *supra* note 1, at 482 n.278; Brief of Amici Curiae Intellectual Property Professors in Support of Bidder's Edge, Supporting Reversal at 17-18, Bidder's Edge, Inc. v. eBay, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (No. 00-15995) (hereinafter "*eBay* brief") ; Brief of Amici Curiae Intellectual Property Professors and Professors of Computer Law, Supporting Reversal at 4, Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (2002), *rev'd* 30 Cal. 4th 1342 (2003) (No. S103781) (hereinafter "*Hamidi* brief"). I recognize that in this footnote I combine an article with two amicus briefs, and that some might argue that the briefs should be evaluated under different standards than the article. I would agree if the briefs were filed on behalf of a client. They were submitted on behalf of the scholars themselves, however, so I treat them as scholarly works.

115 *Compare* Hunter, *supra* note 1, at 482 n.278 (quoting most of the language of comment e through "substantial time," then ending quotation and asserting that "Cyberspace cases on trespass to chattels have ignored this distinction and found trespass to private property even without significant evidence of damage."), *with CompuServe,* 962 F. Supp. at 1023; RESTATEMENT (SECOND) OF TORTS § 218 cmt. 3 (1965).

116 *Hamidi* brief, *supra* note 114, at 4.

117 *eBay* brief, *supra* note114, at 18-19.

118 David Hume, A TREATISE OF HUMAN NATURE 469-70 (L.A. Selby-Bigge, ed., University of Chicago 1978) (1739).

Holmes's aversion to legal dead-hand rule,[119] rhetorically the argument appeals to the reader's inertia and risk aversion. These are real characteristics, but by themselves they do not bear on the merits of any particular claim. The appeal therefore generally tries to give a boost to an argument that can't stand on its logic. (When it does more, one could simply state the case directly and forgo the appeal to inertia and risk aversion, unless they were themselves the basis of some utilitarian argument, which requires more than "it has never been the case" to make.) As I show in the next section, the logic of trespass critique is weak, so this general statement applies well to this particular case.

These partial quotations and appeals to inertia also give an unwarranted boost to the claim that trespasses to land "have always been considered more serious than the equivalent actions against personal property."[120] It is hard to say what "serious" means here, but the *Restatement* makes clear that traditional doctrine thought the two cases should be dealt with in different ways, not that the underlying legal interest in chattel was less important than the underlying interest in land. Indeed, the *Restatement* basically takes it for granted that chattel owners have an interest in inviolable possession, and its casual treatment of the point implies that, under the *Restatement* scheme, trespass to chattel is less serious than trespass to land only in a procedural sense (because owners could take care of chattel themselves), not in terms of the importance of the interest or the perceived severity of violations of that interest.

The failure of the metaphor claim to come to grips with the self-help argument, and the partial quotations in particular, produce a less informative debate than we might otherwise have. I believe that failure can be traced to a misunderstanding in Professor Burk's criticism of the trespass tort.[121] As Part I shows, the *CompuServe* court was the first to use the failure of the self-help privilege to justify extending the cause of action to cover harmless intermeddling.[122] Professor Burk criticizes *CompuServe* extensively, and he argues persuasively that Cyber Promotions' spam did not cause the sort of harm traditionally required to state a cause of action.[123]

However, no doubt accustomed to using the elements of a cause of action as a proxy for the legal interest at stake (the two almost always coincide), Professor Burk did not discuss the court's argument regarding the self-help privilege. Nor did he cite the language the court italicized in ex-

---

119 O.W. Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 469 (1897) ("It is revolting to have no better reason for a rule of law than that so it was laid down in the time of Henry IV. It is still more revolting if the grounds upon which it was laid down have vanished long since, and the rule simply persists from blind imitation of the past.").

120 Hunter, *supra* note 1, at 482. *See also Hamidi* brief, *supra* note 114, at 4; *eBay* brief, *supra* note 114, at 18.

121 Burk, *supra* note 2.

122 *See supra* text accompanying notes 42-45.

123 Burk, *supra* note 2, at 35-36.

plaining its decision to extend the tort. This omission led to an important misunderstanding. The key passage involves Professor Burk's claim that the trespass to chattels tort does not "entail[] the *interest in inviolability* that attends trespass to land."[124] As we have seen, the Restatement acknowledges a "possessor's *interest in the mere inviolability of his chattel*," and states that this interest would be "sufficiently" protected by a privilege to use self-help to prevent even harmless intermeddling.[125] If the legal "interest" in question were not more extensive than the scope of the cause of action, the *Restatement* would not have specified that self-help preserved the interest where the cause of action did not.

This misunderstanding was compounded with Professor Burk's claim that the *CompuServe* court "glibly intermingled trespass to chattels with doctrines related to real property," and thus (with *Thrifty-Tel*) "essentially reversed several hundred years of legal evolution, collapsing the separate doctrines of trespass to land and trespass to chattels back into their single common law progenitor, the action for trespass."[126] Like Professor Burk and the court in *Thrifty-Tel*, however, the *CompuServe* court accurately traced the trespass tort to the conversion tort and used it because conversion did not fit the facts of the case at hand.[127]

For this reason, and because the *Restatement* makes clear that the two torts protect similar interests, it is wrong to say that courts have conflated different legal interests (and different torts), or reversed the path of history. Professor Burk's mistaken propositions have become received wisdom, however, producing two results. First, they taint the entire trespass critique with error. Second, they connect the critique of the trespass tort to the metaphor claim.[128] Professor Burk's claim that courts collapsed the chattels tort into the land tort strongly suggests that judges confused different legal interests, when they had not. The metaphor claim attributes this suggested (but not real) confusion to the use of property-like words, or at least holds that such words confirm the alleged confusion. When the confusion in the trespass critique is cleared away, then, at least to the extent it is based on that language of opinions, the metaphor claim evaporates.

---

124 *Id.* at 33 (emphasis added). *See also id.* (referring to *Thrifty-Tel* and stating that "[c]onflating these two types of trespass has serious consequences; they may share a common history, and even a common name, but they secure entirely different interests"). As noted above, *supra* text accompanying notes 28-34, the claim that the *Thrifty-Tel* court conflated these types of trespass is not supported by the court's opinion.

125 RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965) (emphasis added).

126 Burk, *supra* note 2, at 33. So far as I am aware, the historical status of the *interest* has never been in serious question. *See, e.g.*, Robert Hale, *Coercion and Distribution in a Supposedly Non-Coercive State*, 38 POL. SCI. Q. 470, 471-72 (1923).

127 *CompuServe Inc.*, 962 F. Supp. at 1020.

128 *See, e.g.*, Hunter, *supra* note 1, at 487 (relying on Professor Burk's characterization); Lemley, *supra* note 1, at 527 (same); Lipton, *supra* note 1, at 237 n.6 (same); Madison, *supra* note 1, at 467 (citing Burk).

B. *The Metaphor Claim Diverts Attention from Weaknesses In The Academic Criticism of the Trespass Tort*

Academic criticism of the trespass tort takes two basic forms. The first is the metaphor claim itself. The second is a series of predictions about how extending the trespass tort to the Internet will harm society. In this section, I contend that the trivializing effect of the metaphor claim tends to divert attention from quite serious weaknesses in these predictions. The net effect is to make the predictions seem scarier than they really are. I believe the previous section establishes the trivializing effect of the claim, so to establish this argument I need to show some weaknesses in the academic critique of the trespass tort. I offer five examples of such weaknesses.

The first two examples are from *Hamidi*. The Supreme Court was very impressed by a warning contained in the IP scholars' amicus brief, and echoed in an article by Professor Hunter and a book by Professor Lessig.[129] The scholars' brief warned that, "[u]nder the court of appeals decision, each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel."[130]

As we saw earlier,[131] the court of appeals addressed precisely this argument. Like the *CompuServe* court before it,[132] the court of appeals presumed tacit permission to communicate with systems connected to the Internet, holding only that "where the employer has told the sender the entry is unwanted and the sender persists, the employer's petition for redress is proper."[133] Neither the Court, nor the IP scholars' brief, nor the commentary the Court cited, acknowledged this aspect of the appellate court's opinion. It simply is not mentioned.[134]

---

129 *Hamidi*, 1 Cal. Rptr. 3d at 49.

130 *Id.* (quoting *Hamidi* brief, *supra* note 114, at 14). *See also* Hunter, *supra* note 1, at 508-09 (posing this risk as a rhetorical question); LAWRENCE LESSIG, THE FUTURE OF IDEAS 170 (2001); Burk, *supra* note 2, at 47. In fairness to Professor Lessig, the court cited his discussion of the *eBay* case, which differs in material ways from *Hamidi*.

131 *See supra* text accompanying notes 94-95.

132 *CompuServe Inc.*, 962 F. Supp. at 1023-24.

133 *Hamidi*, 114 Cal. Rptr. 2d at 250. Most of the cases following *CompuServe* involve defendants who persisted in uses to which an owner objected even after the owner notified the defendant of the objection, *see* America Online, Inc. v. IMS, Inc., 24 F. Supp. 2d 548, 549 (E.D. Va. 1998); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1063 (N.D. Cal. 2000); Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382, at *2, *8 (N.D. Cal. Dec. 6, 2001), or in which the defendant does not deny that it had notice of the policy it violated, *see* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 401 (2d Cir. 2004); America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998) (noting steps defendant took to elude AOL filtering software).

134 On top of all that, the scholars' brief elides a distinction between the ends of the network and network elements (servers through which a message might travel) that scholars argue is vital to sensible analysis. *See, e.g.*, LESSIG, *supra* note 130, at 167-68.

A ruling requiring advance permission to send e-mail or browse a website would indeed wreak havoc on the Internet. The metaphor claim, which accuses courts of not understanding the Internet, makes it easy to believe a judge would issue such a foolish ruling. No court has adopted such a rule, however, and the court against which the charge was leveled had explicitly rejected it.[135] Courts have rejected the rule because they understand how the Internet works, not because they are confused.

This argument is weak not only because it attacks a position the appellate court rejected, but because it is counterfactual. Like the *CompuServe* court's similar rule, the appellate court's rule had been in place for some time when the Supreme Court heard the case. No one pointed to examples of the harm that was supposed to occur if the rule was adopted, however. By trivializing judicial reasoning in the trespass cases, and implying (though not stating) that the judges who extended the tort were fools or slaves to real property concepts, the metaphor claim diverts attention from the very serious flaws in this unfounded gloom-and-doom prediction.

My second example has to do with the related claim that extending the trespass tort to Internet cases would render search engines presumptively illegal and reduce social welfare by making it harder to acquire information.[136] The default rule mentioned above rebuts this claim because, under it, searches are presumptively legal until an owner gives notice of an objection. Moreover, and ironically for a claim predicated on the notion that scholars know how the Internet works and courts do not, major search engines already follow a policy of not searching websites that employ a technology known as "robot exclusion headers" to request that search engines search only part of a site or pass it by altogether.[137]

In other words, the criticism does not accurately describe the holdings it criticizes and warns of a state of affairs that already prevails as a matter of Internet norms. Because the state of affairs exists but has not produced

---

135 The closest case to adopting such a rule would be *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 401 (2d Cir. 2004), but the court in that case did not adopt such a rule because Verio admitted it had actual notice of Register.com's conditions and persisted in its conduct anyway. Some comments on this paper insist that if courts enforce any conditions on website use then users will have to examine such conditions before use. *Register.com* does not support that proposition, because the conditions at issue there were contained in replies to queries; they were not posted on the site. Courts that presume that owners consent to all lawful uses of a site simply do not force users to check before browsing. A user that planned to sink a lot of costs into a business model that depended on someone else's site might check first, to avoid the risk that it would be prevented from pursuing its model after a site owner objected to its conduct. It is hard to see what is wrong with that type of negotiation, however. It is just such bargaining that helps owners capture value they create and forces users to bear costs they impose; both effects are socially desirable.

136 *Hamidi* brief, *supra* note 114, at 10-11; LESSIG, *supra* note 130, at 169-71.

137 *See* McGowan, *supra* note 2, at 376 (describing headers). Professor Hunter acknowledges the role these headers play in regulating searches, *supra* note 1, at 505, but he does not discuss the norm when describing how "privatization" threatens the Internet. *Id.* at 508.

the warned-of harm, the warning cannot be right. Moreover, the practice (developed by engineers, not lawyers) of respecting exclusion-header requests not to be searched calls into question how far social practices regarding the Internet diverge from social practices regarding tangible goods. That would be an interesting question to consider, but it has not been considered fully because the fact has not been acknowledged in the debate.

My third example concerns the claim that extending the trespass tort to the Internet would create a precedent that would lead to absurd results. Common examples of such results include broadcasting television or radio signals, which the critique asserts might constitute trespass to television or radio, and sending electric current through a transmission grid, which might conceivably support a claim for trespass to toaster.[138] The basic idea is similar to the problem of a power plant that pollutes the surrounding area through its emissions.[139] The claim asserts that such cases would be actionable under the court of appeals decision in *Hamidi*,[140] though the default rule mentioned above demands at least qualification of that claim.

More importantly, the "trespass to toaster" *reductio* gets the transaction cost structure of the cases backwards.[141] The examples through which the argument is asserted involve a hypothetical defendant dispersing intangibles (electricity or radio waves) over a wide area populated by unrelated persons or, even worse, persons tied to a common electrical grid. If each such person had the right to exclude intangibles from his property then, for any production to occur, all effected persons would have to transfer this right to the producer. The result would be an insurmountable coordination problem, which means no production would occur.[142]

---

138 *Hamidi* brief, *supra* note 114, at 6-7; Burk, *supra* note 2, at 34 & n.56.

139 *Hamidi* brief, *supra* note 114, at 7.

140 *Id.* at 6.

141 There are other examples that get the transaction cost structure right, such as the sending of junk mail and telephone calls. Aside from the role of the government in delivering the mail, it is not clear why injunctions in these cases would be absurd. Courts enjoin one person from calling another all the time, often in harassment or divorce cases. Injunctions in such cases might seem odd if one believed injunctions had some special relationship to tangible property but, as I show in Part III, that belief is archaic.

142 The same fact answers a question Professor Burk posed at the conference where this paper was presented: why couldn't a member of an audience sue a speaker for trespassing on the eardrums of audience members? Disregarding property rights in the classroom itself, if each audience member had a right to be free from sound waves, then for any speech to occur the speaker would have to purchase all the rights, leading to coordination problems and holdouts. The example is weaker than the electricity or broadcast examples, because audience members typically choose to attend lectures and can leave at lower cost than one can leave an electrical grid or broadcast area. One would have to reverse the question to get closer to the Internet case: If one audience member were prohibited from asking questions the lecture could go on and that prohibition would not prevent other audience members from speaking. Taking physical property rights into account weakens the trespass to eardrum case further, because giving audience members a right to be free from sound waves would frustrate the ability of a school to use its rights to exclude to designate certain places for lectures and others as quiet places. Chat rooms

The cases we have examined have just the opposite structure. In each case, the person came to the site or network, rather than the other way around. A defendant either targeted a particular IP address without affecting others' ability to do so, as in *CompuServe* and *Hamidi*, or it had the ability to query some sites and skip others, as in *eBay*. Bilateral bargaining is perfectly possible in such cases; the record in *eBay* shows that it actually occurs.[143]

The transaction cost structure of the cases is vital to choosing between property rules and liability rules. Because this argument gets that structure backwards, it tends to favor liability rules over property rules without engaging the argument for the opposite result. It is no surprise that trespass critics tend to advocate the nuisance cause of action, in which judges perform cost-benefit analysis on their own rather than forcing the parties to do so through bargaining.[144] The metaphor claim makes it hard to see that this argument reverses the transaction cost structure at issue, and obscures the bargaining solution the *eBay* court pursued.

My fourth example concerns Professor Hunter's claim that the metaphorical entailments which cause courts to extend the trespass tort will create an Internet "tragedy of the anti-commons."[145] This term, made popular by the work of Professor Michael Heller,[146] describes a situation where a resource can be used most valuably as a whole but where the law has granted too many people exclusive rights to different interests in the resource.[147] Coordination among conflicting claimants is costly and may be impossible, so the resource may never be used optimally, and may not be used at all.[148]

Coordination is a legitimate concern for the network aspects of the Internet, which is to say the telephone lines and addressing and routing technology that move information from one computer connected to the

---

that impose rules of topicality and decorum provide an online analogy to this point. If chat room hosts could not exclude persons who refused to follow such rules, the room would not serve its particular purpose as well as if the hosts had such a right. *See* McGowan, *supra* note 2, at 361.

143 McGowan, *supra* note 2, at 378-79.

144 *Id.* at 383-84 (discussing scholarly support for the nuisance cause of action). Actually, even the trespass to land tort and the nuisance tort tend to converge in intangible trespass cases. Bradley v. Am. Smelting & Ref. Co., 104 Wash. 2d 677, 684 (1985) ("little of substance remains to any distinction between" trespass and nuisance "when air pollution is involved."). The torts converge largely for the transaction cost reasons the example in the text gets backwards.

145 Hunter, *supra* note 1, at 441-42, 509-13. Actually, Professor Burk was the first to raise this concern, Burk, *supra* note 2, at 49, but Professor Hunter discusses the risk in more detail so I focus on his argument here.

146 Michael A. Heller, *The Tragedy of the Anticommons: Property in Transition From Marx to Markets*, 111 HARV. L. REV. 621 (1998).

147 In his example of Moscow storefronts, "one owner may be endowed initially with the right to sell, another to receive sale revenue, and still others to lease, receive lease revenue, occupy, and determine use." *Id.* at 623.

148 *Id.* at 623-24; Hunter, *supra* note 1, at 502.

Internet to another. The trespass cases deal with the computers at the ends of the network, however, not the "pipes" in the middle, so these cases do not provide a basis for the anti-commons worry. The ends do not have to coordinate for the network to be used.[149] eBay's decision to remain closed, or partially open, does not prevent other sites from making their own choices. In addition, the proposition that "[t]he cyberspace enclosure movement has led to a default principle of exclusion, with a billion unique terms providing the exceptions governing when we can 'enter' these cyberplaces"[150] is not true. As noted above, the *Hamidi* and *CompuServe* courts adopted a default rule of permission, not exclusion.[151]

Professor Hunter believes "the anticommons may be real without our realizing its existence,"[152] which is to say its costs may be opportunity costs we can neither perceive nor measure. I am not sure how this can be. Because the ends of the network do not need to coordinate for the network to function, there is no logical reason to fear the unknown or unknowable anticommons tragedy. In Professor Heller's anticommons model, empty Moscow storefronts exemplified the anticommons problem.[153] With all these chattel cases, where is the Internet equivalent?[154]

More fundamentally, the anticommons risk is only present under conditions that do not hold with respect to sites and networks connected to the Internet. Professor Hunter says "[a]nticommons property emerges where multiple people hold rights of exclusion to *a* property such that no one has an effective right of use."[155] Similarly, Professor Heller describes anticommons property as occurring when "multiple owners hold effective rights of exclusion to *a* scarce resource."[156] Is the Internet, or websites or corporate networks connected to it, "*a* scarce resource?" Hardly. Apart from communications protocols that define what it means to be "on" the Internet, which are not at issue in these debates, it is not "a" single resource at all. Nor, so long as the protocols remain free to use, is it "scarce" in any meaningful sense.[157] (And even if the protocols were owned and restricted, there

---

149 *See* McGowan, *supra* note 2, at 378; LESSIG, *supra* note 130 at 167-68 (acknowledging this point).

150 Hunter, *supra* note 1, at 511.

151 *See supra* text accompanying notes 132-133.

152 Hunter, *supra* note 1, at 512.

153 Heller, *supra* note 146. at 622.

154 Professor Hunter suggests auction aggregators will be hurt by decisions such as *eBay* though, as I note in the next argument, he does not consider all the costs and benefits of the activity at issue in that case. This claim does not explain why auction aggregators eBay allowed to perform real-time queries would go under, unless their business models just didn't make sense in the first place. The claim that search engines will be harmed seems to me unsupported by the facts.

155 Hunter, *supra* note 1, at 444 (emphasis added).

156 Heller, *supra* note 146, at 673 (emphasis added).

157 Lemley, *supra* note 1, at 534-35. In this regard it is telling that when trespass critiques make the anticommons argument they do so by treating all technologies relevant to the Internet the same.

would be no anticommons tragedy unless ownership in the protocols was fragmented.)

It is therefore no surprise that Professor Hunter shifts from the singular to the plural when describing the anticommons tragedy he predicts: "no one will be allowed to access others' cyberspace `assets' without using some form of licensing or other transactionally expensive permission mechanism."[158] Where in this statement is there anything about a scarce resource that is under-utilized because it is subject to rights to exclude held by many different people? The (many) assets of (many) others are not a scarce resource subject to conflicting rights.[159] This fact may explain why he does not predict a true Internet anticommons, saying only that "splintering of access rights is analogous to the overlapping rights on the Moscow street. Because of it, we no longer have a right to access the commons property."[160] What is the analogy? The Moscow example involved a scarce resource that could not be put to optimal use; this statement complains of a resource one has to obtain consent to use, which is a very different thing. This is just a pricing system.[161]

At one point Professor Hunter defines "the `property' at issue not as individual websites or email systems, but rather "the commons property of the network resources: the Web or the email system that we all used to share."[162] It is not at all clear what this statement means.[163] It is clear, how-

---

Thus Professor Burk's rhetorical suggestion that "one can imagine the anti-commons nightmare that could ensue on the Internet in web linking, indexing, and other routine functions if every owner of equipment attached to the network were granted a cause of action for the trespass of unwanted electrons on her equipment." Burk, *supra* note 2, at 49. Professor Lemley also invokes network elements in discussing the anticommons argument, though he draws some distinctions between, for example, top-level domains and second-level domains. *See* Lemley, *supra* note 1 at 534-35. In other circumstances, however, scholars insist on distinguishing between the ends of the network and technology in the middle, *see* Larry Lessig and Mark A. Lemley, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era* , 48 U.C.L.A. L. REV. 925, 930-31 (2001), and that distinction applies readily to the trespass cases, all of which are about the ends, not the middle. Professor Burk makes a good and important point about technology comprising the "pipes," but that is not what the cases are about.

158 Hunter, *supra* note 1, at 446.

159 My thanks to Richard Epstein for emphasizing this point.

160 Hunter, *supra* note 1 at 511.

161 I think the real core of the objection to these cases takes the form of the claim that the cost of the pricing system—which is indeed positive—exceeds the value the system creates, in the form of internalized externalities, the information provided by prices, and so on. That is a cogent claim, which might or might not be right, but it has nothing whatever to do with the doctrinal arguments or the parade of horribles asserted in these cases.

162 Hunter, *supra* note 1 at 511.

163 Taken literally, I suppose, it proposes that everything connected to the Internet is, by some sort of stipulation, a single resource, with the result that sites should not be allowed to password protect their content, or safeguard credit card information, and so on, so that we all can "share" the information in the single common of the Internet. I am not aware of anyone who proposes such a rule for Internet regula-

ever, that the cases are not about such a broad amorphous concept. Hamidi did not sue for access to "the Web or email system that we all used to share," he sued for access to Intel, and had he been enjoined from sending e-mail to Intel employees he still would have had his own webpage and the ability to email employees individually. Bidder's Edge did not want to spider the Web generally, but a specific site on which much of its business model rested. The anticommons rhetoric turns out to be a grossly inapt metaphor that has nothing to do with actual cases.[164]

It is true that potential users with notice of a limitation might be expected to follow that limitation, and that courts in trespass cases will have to match the required notice to the type of user (i.e., conspicuous English for persons, technologically appropriate means for bots), but it is not clear that this rule has caused any harm at all. A majority of cases have followed it, including the Second Circuit (applying New York law);[165] where is the harm?[166] It would be interesting to discuss public policy implications of particular terms, as we do in contract law, but that discussion has not happened, in part because the metaphor claim gets in the way.

The point may be the more modest one that society would be better off if the trespass tort were not extended. There is nothing logically wrong with such a claim, but the metaphor claim makes it harder to get at this point and obscures the fact that the economic approach implied by courts

---

tion, *see* McGowan, *supra* note 2, at 368-69, and I do not read Professor Hunter as supporting such a rule.

164 At best, one could argue that the anticommons point might be defended on the ground that a distinction between network elements and the "ends" of the network is misleading. Drawing on the "layers principle" discussed by Professors Solum and Chung, one might argue that the cases involve different (but unitary) technical protocols: SMTP, in the case of *Hamidi*, and HTTP, in the case of *eBay*. *See* Lawrence B. Solum and Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME. L. REV. 815 (2004). Even stated this way, however, the anticommons argument fails, because the choice of one site or network owner to block data or requests for data from particular sources does not reduce the utility of the protocol to other users who do not wish to block anything. In fact, even if one shut down a server that served to transmit data between different parties (as might happen if Intel's servers acted to relay data unrelated to Intel), the Internet protocol would route around any blockage, so the shutdown would not create the gridlock the anticommons argument worries about. Indeed, a moment's reflection reveals the absurdity of this line of argument. Some of the research that now helps comprise the Internet was motivated by a desire to build a communications network that could survive nuclear attack, *see* Paul Baran, *Introduction to Distributed Communications Network*, Rand 1964, available at http://www.rand.org/publications/RM/RM3420/. This idea would have been pointless if anticommons premises applied to the Internet.

165 Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).

166 Professor Hunter believes only a few sites practice exclusion, though he presents no data on this point. Hunter, *supra* note 1, at 511. I am not aware of any hard numbers either, though if business reasons cause firms to remain open I am not sure why granting rights will cause the harm he predicts. *Cf.* McGowan, *supra* note 2, at 371 (noting economic incentives for sites to remain open). If a site wishes to be browsed or employed to send e-mail, there will be no dispute. The policy question is how best to equilibrate costs and benefits when the managers of a site object to particular uses of information (in browsing cases) or information processing capabilities (in unwanted email cases).

extending the tort—property rights and bargaining—might at least offer a crude *net* welfare measurement. Neither the metaphor claim nor the trespass critique offers anything other than the hope that judges will do the job better than parties.[167] No doubt one could advance affirmative reasons for that view, but the largely negative attack of the metaphor claim and the trespass critique does not advance them.

My fifth example concerns the costs and benefits of disseminating information. The IP scholars' brief in *eBay* argued that the trespass tort would reduce social welfare because it would place search engines at the mercy of site owners and limit the degree to which the Internet distributed information.[168] Because search engines skip sites when requested already,[169] the claim is overstated, but the conceptual point is important. The scholars warned of firms like eBay leveraging market power, and praised the positive effects of disseminating information. These are valid concerns.

What if the information causes harm, however? eBay's story was that "bids beget bidding," meaning that bidders are more likely to bid on items other bidders have bid on already. Because the state of bidding on an item might signal the desirability of that item, sellers had an interest in ensuring that only accurate (timely) bid price data were disseminated to the market. eBay worried that that Bidder's Edge harmed its sellers by posting outdated price information.[170]

My point is not that eBay was right about all this—it may or may not have been. My point is that, as Judge Posner and Professor Landes have recently stressed,[171] not all "information" effects are positive. Sometimes the distribution of information causes harm. When it does, such harm counts in the social welfare function and has to be evaluated relative to whatever benefits the distribution yields. Even this relatively strong critique of the trespass tort suffers from its inability to measure *net* welfare effects.

---

167 McGowan, *supra* note 2, at 383.

168 *eBay* brief, *supra* note 114, at 4-7. On the leverage and competition theories, *see supra* notes 50 and 70.

169 *See supra* note 137.

170 McGowan, *supra* note 2 at 381-82. Some comments on this paper suggest trespass would not be the right tool to address this issue, but I don't see why not. Claims for misrepresentation might or might not work—if the aggregator said nothing about the age of the data it would not be lying, and I don't see why it would have a duty to disclose its search methodology. In any event, overlapping causes of action are common and it makes no sense to get caught up in arguments about which tort to use rather than the sort of straightforward institutional utilitarianism required to decide whether judges or parties should equilibrate costs and benefits in such cases.

171 William L. Landes & Richard A. Posner, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 221-25 (2003); *see also* Stan Liebowitz and Stephen Margolis, *Seventeen Famous Economists Weigh in on Copyright* (December 2003) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=488085) (arguing that economists brief against copyright term extension did not account for role of copyright in internalizing externalities).

In *eBay,* one could follow the district court and rely on bargaining, or one could follow the trespass critics and let judges use litigation to weigh costs and benefits. That option interjects judges into essentially managerial decisions; they have to decide whether bids really do beget bidding or, if the evidence is inconclusive, whether that is likely. I prefer bargaining to judicial oversight because it is not hard in this sort of case, as evidenced by the fact that it occurs in at least some cases, but I admit that neither bargaining nor judicial oversight is perfect. My point here is not that the trespass critique is wrong (though I do think it is), but that it has serious problems of its own, and that the metaphor claim diverts attention from those problems. The result is a less informed and less informative debate.

III

My final argument is that the metaphor claim and criticisms of the trespass tort are tied far more closely to traditional, physical-world notions of property than the opinions they criticize. For this reason, the metaphor claim applies better to those who advance it, and who criticize the extension of the trespass tort, than to those at whom the claim is directed.

Metaphor claimants and trespass critics all concede that harm to hardware can support a cause of action. They deny that other forms of harm, such as the value of the business that runs on the hardware, should support a cause of action.[172] The *Hamidi* court agreed.[173] No serious cost-benefit analysis would ignore losses just because no hardware was hurt, however.[174] Metaphor claimants and trespass critics know that. Why then do they insist that only harm to hardware should state a claim? The IP scholars' brief in *Hamidi* suggests an answer: "[a]bsent the requirement of harm to the chattel itself, the doctrine of trespass to chattels takes on absurdly broad dimensions."[175]

Why absurd? As usual with argument by adjective, the key is to ask what idea the term is supposed to express. This sentence ties the legal notion of "property" to things like dirt (realty) or tangibles (like hard drives),

---

172 Burk, *supra* note 2, at 36-37; Hunter, *supra* note 1, at 487; Lemley, *supra* note 1, at 527 n.25; Madison, *supra* note 1, at 469-70; *Hamidi* brief, *supra* note 114, at 4-5.

173 *See supra* text accompanying note 106.

174 One might equally well ask what is so special about harm to hardware, such as crashing a server? Other than tradition, what justifies a cause of action for such harm when the server is connected to the "commons" of the Internet? After all, as one dissent in *Hamidi* pointed out, no particular user could know what load a system was under at any given point in time, and thus could be responsible for crashing a system when most of the capacity was taken up by others. 1 Cal. Rptr. 3d 32, 74 (Mosk, J., dissenting). Such claims are justified in the right circumstances; my point is that by taking them for granted metaphor claimants and trespass critics avoid comprehensive analysis, which justifies claims in cases such as *Compuserve* and *Hamidi*, too.

175 *Hamidi* brief, *supra* note 114, at 5.

and insists that it would be absurd to sever the tie. The whole trend of 20th Century property theory, however, has been just the opposite. Scholars have made sense of the notion of property by insisting that it has no inherent or intrinsic relation to things, and instead must be analyzed in terms of relations among persons with regard to things. According to Professors Thomas Merrill and Henry Smith (who criticize the trend they identify), the modern view of property is that it is "a composite of legal relations that holds between persons and only secondarily or incidentally involves a "'thing.'"[176]

Professors Merrill and Smith believe economic analysis, and particularly the transaction cost analysis of Professor Ronald Coase, "gave rise to a conception of property as a cluster of in personam rights and hastened the demise of the in rem conception of property."[177] They believe the demise of the *in rem* conception was essentially completed in Professor Calabresi and Melamed's discussion of "property" rules as opposed to liability rules, a discussion in which the concept of property was simply a policy tool bearing no relationship to any particular "thing."[178] As Professor Emily Sherwin puts it, "from Hohfeld and Coase it is an easy step to say that property rights are simply rights, to which the term 'property' adds nothing at all."[179]

Because most judges are accustomed to using "property" to designate a certain type of right, the use of that word does not betray a misunderstanding of the Internet or a fixation on things. In fact, if and to the extent the term "property" no longer designates tangible things as much as it does the rights and obligations of persons, then the linguistic component of the metaphor claim falls apart completely. The purely cognitive aspect of Professor Hunter's argument suffers, too, because the trend away from *in rem* conceptions of property is at odds with the claim that metaphors constrain thinking. If property metaphors did not stop judges from severing rights from things, why would those metaphors entail anything about the Internet?

---

176 Thomas W. Merrill and Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357, 357-58 (2001). Their objections do not apply to the trespass cases because they believe tying property to things economizes on information costs by giving persons a standard-form expectation of how they should deal with things they encounter. *Id.* at 386-88. Where users come knowingly to the resource, however, as in every Internet trespass case, they already have some knowledge of what the resource is and what they would like to do with it. What they need, according to Professors Merrill and Smith, is a clear understanding of the rules. The property approach does a better job of settling expectations than having judges run websites through *ex post* cost-benefit analysis under the nuisance doctrine, which is what trespass critics seem to prefer. *Hamidi* brief, *supra* note 93 at 7-8.

177 Merrill & Smith, *supra* note 176, at 360-65. The reference is of courts to the classic relation of bargaining to property rules and liability rules, Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972).

178 *Id.* at 380.

179 Emily Sherwin, *Two-and-Three-Dimensional Property Rights*, 29 ARIZ. ST. L.J. 1075, 1078 (1997).

In contrast, with their insistence that trespass causes of action be tied to harm to tangible things, metaphor claimants and trespass critics express an *in rem* vision of property and reject the view of property rights as just "rights" that order human interaction. It is no surprise that the *Hamidi* brief supports its claim of absurdity with the trespass-to-toaster *reductio* which, as we saw in Part II, focuses on physical aspects of networks such as electrical grids and gets the transaction cost analysis exactly backwards. The unit of analysis in transaction-cost economics is the transaction, which is to say an interaction between human beings, not a thing. The backwardness of the toaster example suggests that metaphor claimants and trespass critics are focusing on the wrong thing. Their insistence on the thing-ness of property has diverted their attention from what people do with and to each other with regard to those things.

This analysis supports a conjecture: Behind the metaphor claim lies an atavistic notion of property. This vision obscures analysis of the costs and benefits of human behavior, which is why over the last 40 years legal analysis has discarded it. Modern property theory is right to focus on persons and their interactions, and thus on truly *social* costs and benefits, rather than on things as such.[180] The most important question is whether society is better off allowing site and network owners the presumptive right to exclude others from using the owners' systems to send or retrieve data, or whether it would be better for users to have a presumptive right to use.

Once one answers that question, picking a doctrine to generate the desired rule is in one sense a detail. One could build an analytical bridge from this decision to whatever doctrine seemed best suited to support it.[181] Trespass to chattels has served this purpose in the cases we have examined, but that fact is really incidental to the choice of default rule. All the talk of doctrinal formalism and harm to chattel is therefore beside the point. Insofar as property is concerned, metaphor claimants who worry that a blinkered focus on physical property will distort analysis of Internet issues are right. With Pogo, they may truly say that they have met the enemy, and it is them.

I believe this analysis plausibly explains much of the academic opposition to extending the trespass tort. It accounts for the "it-has-always-been-that-way" line of argument, which opposes what in fact is a quite ordinary judicial adaptation of common-law principles to meet changed circumstances. This analysis also suggests two further points regarding debates over Internet regulation. The first point concerns the proper subject of legal analysis. That the metaphor claim rests on an unacknowledged *in rem* con-

---

[180] It is interesting to ask what makes a thing a thing. One answer, suggested by Professor Henry Smith at the conference where this article was presented, is for legal purposes a "thing" is created by awarding a right to exclude—it is in this sense a byproduct of the allocation of rights analysis.

[181] Some doctrines may help guide analysis more than others, so there is a sense in which the doctrinal bed is important, but it is important as a guide to analysis, not for its own sake.

ception of property suggests that it also either rests on or is compatible with the view that technology, rather than people, is the proper subject of legal analysis. One can see this view, for example, in the argument from *Hamidi* that, in processing data, computers are simply doing what it they were "intended" to do, or just operating "normally."[182] One can understand how a person holding this view would be infuriated by the frequent judicial discussions of bandwidth or disk space, and the courts' fanciful worries about harm to hardware, which (on the facts of these cases) is so unlikely that its expected cost is trivial.[183]

Law cannot regulate things, however. It can only regulate people. There is no law of the "Internet" any more than there is a law of the bicycle, the backhoe, or the three-pronged rake.[184] To focus on technology as such, rather than as a fact relevant to certain human interactions, is to take one's eye off the ball. It may well be the case that human interactions on the Internet call for changes in the law because the Internet allows people to do new and different things to and with each other, or because the old things they do have different consequences in cyberspace. It is not the case that this fact means the law can regulate technology rather than people, so it is not the case that the law should focus on technology rather than what people do.[185]

The second point concerns the rhetoric of current academic debates over intellectual property and Internet regulation. The arguments we have examined in this Article, like much criticism of recent copyright legislation, "shrinkwrap" licenses, digital rights management, and other measures designed to maintain property and contract as the basis for "information" transactions,[186] draw heavily on classic Legal Realist themes. These include

---

182 Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1360 (2003) (claiming Intel's system merely worked as designed); *Hamidi* brief, *supra* note 114, at 5-7.

183 *See supra* text accompanying note 65; *see also* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, (2d Cir. 1994) (affirming trial court injunction based on fanciful risk of harm if conduct at issue were multiplied).

184 This point is related to but distinct from the debate between Judge Easterbrook and Professor Lessig over whether "cyberspace" would be a meaningful subject of legal analysis, or a shallow category unworthy of separate study, such as the hypothetical "law of the horse." Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999). The question in this debate was whether studying "cyberlaw" would yield general insights regarding the law. The point in the text is that, if one were to try studying "cyberlaw," it would be better to keep one's eye on what people were doing with technology than on the technology itself.

185 The law can of course order people to construct technology in a way that constrains the choices of other people, as in Professor Dan Burk's example of a car that will not start until seatbelts are in place. The law cannot order the belt to do anything itself, of course, it can only order those who build cars to build them in a way that constrains the choice to drive unbelted.

186 *E.g.* Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 44 (2001).

a tendency to collapse the public-private distinction,[187] worry about private economic power and "private legislation,"[188] and insist that property and contract are socially constructed concepts that may be altered to suit the needs of society.[189] All these points are right to some extent, and to read this work is to be reminded of the work of Robert Hale (which I mean as a compliment).[190]

It was of course a fundamental point of the Realist critique that law must be analyzed as lived reality rather than as formal, abstract principles.[191] History and tradition cut little weight in this analysis. Why, then, do we see the sorts of arguments we have analyzed in this article? I do not think it is because scholars who advance the metaphor claim, criticize extension of the trespass tort, and decry the "enclosure" of the Internet are actually wedded to the formalistic severing of remedies from legal interests, or to "it-has-always-been-that-way" arguments.[192]

Instead, a large part of the answer is that many IP scholars have translated Realist insights into the more refined language of law and economics. These scholars assert that nonrivalrous consumption implies that there are few if any negative externalities to dealings with "information," and that it is socially undesirable to internalize all positive externalities, so copyright terms should be short, shrinkwraps should be gutted or rewritten as needed, spammers and browsers should be free to do as they will, digital rights

---

187 As implicit in Larry Lessig's equation of legal and market "regulation," and his more general thesis that code is law. *See* Lessig, *supra* note 184, at 509. Professor Lessig makes the point explicit with his dictum that "private law is oxymoronic," *id.* at 530, for which he cites Morris R. Cohen, The Basis of Contract, 46 HARV. L. REV. 553, 585-92 (1933); Morris R. Cohen, Property and Sovereignty, 13 CORNELL L.Q. 8, 21-30 (1927); and Robert L. Hale, Bargaining, Duress, and Economic Liberty, 43 COLUM. L. REV. 603, 626-28 (1943); and Robert L. Hale, Coercion and Distribution in a Supposedly Non-Coercive State, 38 POL. SCI. Q. 470, 488-91 (1923). Lessig, *supra* noted 184, at 530 n.197.

188 *See* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1274 (1996) (citing Friedrich Kessler, *Contracts of Adhesion -- Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943)).

189 *E.g.* Julie Cohen, *Lochner in Cyberspace, The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 494-95 (1998) ("Declarations of entitlement are definitional, public acts and should be understood as such"); citing Felix S. Cohen, Transcendental Nonsense and the Functional Approach, 35 COLUM. L. REV. 809 (1935); Morris R. Cohen, *supra* note 171; Hale, *Coercion*, *supra* note 171.

190 Though I don't think he was right when he laid out his own case. *See* Richard Epstein: *The Assault That Failed: The Progressive Critique of Laissez-Faire*, 97 MICH. L. REV. 1697 (1999).

191 Or, "transcendental nonsense," if you will.

192 Nor is it devotion to judicial restraint. Many of the same scholars who advance the metaphor claim and oppose extension of the trespass tort also argued that the Supreme Court should have struck down the Copyright Term Extension Act, which would have required a fairly aggressive and creative assertion of judicial power.

management must allow for fair use, and intermediaries such as Napster or Grokster should not be liable for the copying they enable.[193]

The initial rhetorical move in modern IP debates, in other words, is for IP critics to seize the magic words of utilitarianism.[194] This strategy works for those who believe these arguments are sound, as well as those who dislike economics but believe these arguments are useful. The problem with this move is the same problem the Realists faced when they got past insisting that economic rules were matters of policy within the domain of the legislature, not eternal truths etched into the Constitution: It is very hard to measure net utility, and when measurements run out you find yourself making the sort of ideologically charged arguments (or interpretations of ambiguous data) you accuse your opponents of making, just for a different ideology.

That point is easy to see with regard to the cyberspace trespass to chattels cases. The claim that net social welfare will suffer if courts opt for property rules in cyberspace is too hard to prove. Worse yet, the trespass critique does not even offer a means of measuring the net utility of particular interactions. Ordinarily, consent to an interaction justifies an inference that the interaction generates positive net utility. The trespass critique largely eliminates the basis for that inference. It instead collapses the idea of consent into a decision to make content available online and a decision not to password-protect. All interactions after these two decisions are presumed to generate positive net utility, unless a site owner convinces a judge that a particular practice should be condemned as a nuisance. The critique offers no justification for this assumption, however, not even at the level of a behavioral assumption.

It is therefore hard to take seriously the general welfare claim of the trespass critique. The more specific claim that the sky will fall if courts enjoin spamming or browsing is illogical and, more importantly, is falsifiable and has proved false. The consequentialist line of attack on these cases therefore leaves something to be desired. That being the case, it is perhaps no surprise to see very formal doctrinal arguments. And if one believes it would be absurd to extend the idea of "property" beyond tangible "things," then judges who think something else might well seem confused. (It is also easy to see how a critic of current IP policy might savor the chance to play the judicial restraint card *against* large commercial entities such as Intel or eBay.)

The problem with *that* move, of course, is that it still does not answer the question of why courts should favor data harvesters and spammers over

---

193 For a survey of such positions, *see* Lawrence Lessig, FREE CULTURE (2004); Lessig, *supra* n.130. For summary for purposes of critique, *see* Frank H. Easterbrook, *Cyberspace Versus Property Law?*, 4 TEX. REV. L. & POL. 103, 104 (1999).

194 *Cf* Stanley Fish, THE TROUBLE WITH PRINCIPLE 309 (1999) (recounting how "the right hijacked the magic words").

web site operators and owners of internal networks connected to the Internet. The metaphor claim helps cover this analytical gap by (wrongly) depicting judges as confused or constrained, implying that their decisions are confused and therefore wrong, but the claim does nothing to actually close the gap. It is weak to the extent it is not false, and it leads to a rhetorical dead end. It would be better to get rid of it.

CONCLUSION

The trespass topic provides a wonderful context for debating Internet governance. The debate has been less interesting than it might be, however, because of the muddle I have tried to clear up here. The preceding discussion suggests some recommendations for improving that debate. The main points are as follows.

First, courts in the cases we have discussed have not ignored differences between the Internet and the physical world, and there is little if any reason to believe they have been misled by words. It is truer to say the judges' reasons have gone unnoticed than it is to say the judges have missed any important points. The metaphor claim and the trespass critique condescend to these judges by implying that their decisions are foolish, and appearing magnanimously to attribute this foolishness to confusion or constraint rather than stupidity, while never coming to grips with the reasons judges have advanced for their decisions.

Second, the metaphor claim rests mainly on confusion about the trespass tort. The confusion stems from the premise that chattel owners have no legal interest in the inviolable possession of chattel. That premise is wrong, and any argument that relies on it is unsound. That premise is the source of the claim that courts extending the trespass to chattels tort are in some sense "really" applying the tort of trespass to land. That claim, too, is wrong.

Third, two practices common to the debate are undesirable. The first is the practice of partially quoting comment e to Restatement Section 218 and omitting the last sentence of the comment, on which cases extending the tort have relied. The second is the practice of claiming that courts in trespass to chattels cases have adopted rules demanding advance permission to browse a website or send an e-mail, while not acknowledging opinions, such as in *CompuServe* and *Hamidi*, which do the opposite. The first practice is misleading, and the second is a straw-man argument that bespeaks weakness in the claim it is advanced to support. Both practices are unfair to courts and make it hard to engage in practical debates over the welfare effects of different default rules.

Fourth, though the preceding recommendations will improve the clarity and candor of the discussion, everyone should acknowledge that the black-letter doctrine is secondary to normative considerations. The debate should focus on what matters instead of what does not. For utilitarians that

means a straightforward cost-benefit analysis of different rules rather than a focus on *in rem* notions of property. It also means acknowledging that activities involving "information" can create economic costs as well as benefits, even when those activities do not harm hardware. The debate should consist of arguments about how best to net out these effects, rather accusations about one side of the equation followed by a *non sequitur* proclamation that the netting is done. The real choice is whether judges, legislatures, or parties should equilibrate those costs and benefits. I have argued elsewhere that it should be the parties; my point here is that this is the debate we should be having, rather than worrying over metaphors or the prospect of doctrinal evolution.

Fifth, utilitarian analysis is bound to leave some questions open. Different analysts will answer those questions in different ways. Because the answers by definition cannot come from utilitarian analysis, they have to come from somewhere else. I have argued in other work that they come from the different ethical commitments of different analysts.[195] That point applies to trespass cases, and the metaphor claim that muddles them, as well as to any other issue. The best reason to reject the claim is so that we can engage in clearer analysis of the complex combination of instrumental and normative considerations that determine actual policy.

---

195 David McGowan, *Copyright Nonconsequentialism*, 60 MO. L. REV. 1 (2004).

INTEL v. HAMIDI: THE ROLE OF SELF-HELP IN CYBERSPACE?

Richard A. Epstein[*]

I. THE ASSAULT ON THE INTERNET

In my initial contribution to this volume, I developed a general framework for analyzing the use and limits of the self-help remedy. One central conclusion of that paper was that the transition from the state of nature to civil society carried with it one major advantage. It allowed everyone—plaintiffs and defendants alike—to replace an uncertain and often capricious system of self-help with more certain legal remedies administered by neutral state officials. Ubi ius, ibi remedium: where there is a right, there is a remedy. In some cases, that legal remedy will be of sufficient strength that it entirely displaces a flawed self-help remedy. In other cases, the legal remedy works as a supplement to self-help, allowing the individual to choose between them.

Unfortunately, it is all too clear that legal remedies in cyberspace are often fitful and unreliable, which places more stress on the self-help remedies that so many papers in this volume examine. In this paper, I do not address the question of when self-help is allowed because legal remedies fail. Rather, I turn to the converse question: whether the state should *ever* deny a legal remedy against the wrongdoer when the system of self-help breaks down. The stakes here are high. It is now understood that the greatest challenge to the integrity of the Worldwide Web stems from its unique advantage: its well-nigh infinite connectivity. Before the Web, computers were stand-alone machines that functioned as glorified typewriters and number crunchers. Their ever-more rapid speed of operation did not, by itself, create a social network. But email and the web allow any two people to be brought into instant, if anonymous, contact with each other. That end-to-end network generates huge social benefits too obvious to elaborate here.

---

* James Parker Hall Distinguished Service Professor of Law, The University of Chicago; Peter and Kirsten Senior Fellow, The Hoover Institution. My thanks to Alix Weisfeld, class of 2006, for her valuable research assistance. I should like to state at the outset that the views in this paper are entirely my own, and do not represent those of Intel Corporation. I entered the case only when Intel v. Hamidi was before the California Supreme Court, long after the basic issues in this case were defined, and had no role in developing the theories on which the case was initially tried. I was the author of the Amicus Curiae Brief submitted on behalf of various industry groups in support of Intel. I defend many of the arguments made in that brief in this article.

But the flip side is that this same connectivity propagates the spread of viruses, hackers,[1] and, most relevant to this paper, spam.[2]

Looking at the severity of threats to the Internet, we must resist the temptation to say that many users of the system are rogues and knaves.[3] In reality, the opposite is true. At a guess, 99.99 percent of Internet users are law-abiding individuals who respect the usual conventions for communication. But what is notable is that the remaining 0.01 percent is capable of disrupting the entire system. Today, some estimates put spam above 80 percent of the total traffic, at around 260 billion pieces in 2002, and growing rapidly.[4] Laments aside, it seems pointless to recite the huge social and private costs that come from the heroic but imperfect efforts that users and Internet service providers take to filter spam, or to lament the ineffectiveness of the CAN-SPAM Act, whose most notable feature is its klutzy acronym.[5] Today, each effort to place clever filters on email inspires new efforts by spammers to elude them in an endless arms war.[6] Here the risk is not that self-help mechanisms will involve the excessive use of force against spammers or against third persons. There are few cases of wrecking the computers of spammers on record.[7] Self-help is often unable to complete the job, leaving a crucial place for legal remedies, both civil and criminal, that take direct aim at the perpetrators by damages and injunctive relief.

II. *INTEL CORP. V. HAMIDI*—AGAIN

The issue then arises whether the courts will be prepared to issue these legal remedies. The problem has come to a head in a case that has become an instant legal classic: *Intel Corp. v. Hamidi*,[8] in which the California Su-

---

[1] For further discussion, see Randal C. Picker, Cybersecurity: Of Heterogeneity and Autarky (forthcoming, 2005, The Law and Economics of Cybersecurity, eds. F. Parisi and M. Grady, Cambridge Univ Press)(noting the widespread use of zombie computers to spread spam).

[2] For the origins of this term (which once referred to Hormel preserved meats), see Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY. TECH. L.J. 625, 631-632 (2004).

[3] For discussion, see Richard A. Epstein, *The Theory and Practice of Self-Help*, 1 J.L. ECON. & POL'Y (2005).

[4] Mossoff, *supra* at 627 ("I am in the habit of counting spam-only mornings, where all the email from overnight is spam.")

[5] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701 – 7713 (2003). For an account of its provisions, and their futility, see Mossoff, *supra* at 634-640.

[6] Mossoff, *supra* at 632-634 (discussing the "folly of filters").

[7] For one such, see Bruce Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y (2005).

[8] Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003). I have already written about this decision before the final decision in the California Supreme Court. See Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73 (2003). The decision has also brought forth many articles on the subject. *See, e.g.*, Dan Hunter, *Cyberspace As Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003);

preme Court held by a narrow 4 to 3 margin that the ancient rules of trespass to chattels blocked the use of injunctive relief against the defendant who sent unwanted messages through the plaintiff's servers after being explicitly told by its owner not to do so.

The facts of the case, briefly stated, are these. The defendant Hamidi was a former employee of Intel whom the firm fired in 1995. The dismissal itself was acrimonious, and resulted in a workman's compensation claim by Hamidi, which the local workers' compensation panel dismissed on the grounds of fraud. Stung by his defeat, in 1996, Hamidi organized an anti-Intel web site and organization, FACE-Intel, whose stated purpose was to function as an "opposition group" to expose what Hamidi perceived to be the shortcomings of Intel's employment practices. Hamidi maintained a web-site that outlined his charges, which was accessible to present and former Intel employers. But he also sent on several occasions inflammatory emails to large groups of Intel employees—as many as 35,000 at one time—berating the company for its practices. In so doing, he made unauthorized use of Intel's servers to distribute the information. The emails in question placed no strain on Intel's capacity to process its own work. They were, standing alone, too infrequent to do that. But they did create consternation and uneasiness within the ranks, which took a good deal of time to respond to. On several occasions, Intel specifically requested that Hamidi stop sending his message through its server, but he refused to do so. Intel tried to set up filters to block the messages, but these were, as they always are, easily evaded by a determined intruder.

At this point, legal relief seemed in the air. Intel could have sued, and perhaps won, a suit for defamation against Hamidi, but that action would have required an examination of the truth of his explosive allegations, its impact on numerous employees, and perhaps the mental state of the defendant, as well as some questions of possible privilege. As veterans of the defamation wars well know, this was not an appetizing prospect, for it required republishing the very charges whose impact Intel sought to minimize. The suit for trespass to chattels, in which only injunctive relief was requested, avoids those difficulties by asking for less. The gist of the complaint was the invasion of the machines and the use of the equipment, not the content of the message. As Intel framed its argument, the case was easier to prove but even if it were fully successful, Hamidi could still continue to post his inflammatory messages on his own website or otherwise communicate them to Intel employees.

My own rooting interest in this case stems, as previously noted, from my role as the author of an amici curiae brief for Intel. I was criticized by name in Justice Werdegar's forceful but misguided majority opinion, which

---

Mark A. Lemley, *Place and Cyberplace*, 91 CAL. L. REV. 521 (2003); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433 (2003); David McGowan, *The Trespass Trouble and the Metaphor Muddle*, 1 J.L. ECON. & POL'Y (2005).

denied Intel the injunctive relief that had been granted it below. Werdergar begins her argument by affirming the simple rule that an actionable trespass for chattels requires the proof of actual damages. Here the relevant text is the Restatement (Second) of Torts, which reads as follows.

> 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 a chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, 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, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c) [relating to the deprivation of use for a substantial time]. Sufficient legal protection ... of his chattel is afforded by his privilege to use reasonable force to protect his protection against even harmless interference.[9]

The Restatement's only illustration of nominal damages reads in full: "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."[10]

The Restatement provision here does not deny that the trespass has taken place. It only denies that some trespasses to chattels are *actionable*. The property rights in chattels are said to be inviolate, and self-help, with its usual caveats about reasonable force, is said to supply the sufficient remedy in the absence of the specific forms of harm mentioned in the section. The sole illustration offered shows that, historically, the only cases to which this rule has applied are those for which no one would choose to bring an action at all. Just take the dog home. Here the Restatement works well because if the defendant persists in the conduct, then the recurrence of harm makes an injunction available. This rule for chattels, for which there is virtually no case authority, differs from the rule that governs trespass to real property. There the inviolate nature of the owner's interest implies that its owner can always secure a legal remedy against any invasion of land, however small, if only to guard against the creation of an easement.[11] For real property, all trespasses are not only wrongful; they are always actionable.

In dealing with this particular case, Werdegar argues that this damage requirement cannot be evaded by pitching the claim as demanding only injunctive relief, because that only raises the bar that the harm in question

---

9 RST § 218, Comment *e*:

10 Restatement (Second) of Torts, § 218, cmt. e, illus. 2 (1965).

11 Dougherty v. Stepp, 18 N.C. 371 (1835) ("[I]t is an elementary principle, that every unauthorised, and therefore unlawful entry, into the close of another, is a trespass. From every such entry against the will of the possessor, the law infers some damage; if nothing more, the treading down the grass or the herbage, or as here, the shrubbery.").

be not only actionable, but also irreparable. She contrasts Hamidi's emails with that of spam where the inundation of material causes the machines to slow down (which happens less as their capacity increases) or requires excess time by users to delete the message in question. To her, the decisive difference was that the workers for Intel were distracted by the *content* of the messages, not by their frequency. But objections to content interests don't count as interests protected by the tort of trespass to chattels.

There are two responses to this line of argument. First, the question is why stick to the rule that requires a proof of actual damages in order to obtain injunctive relief? Here Justice Werdegar conceded that the self-help remedy was available, so that if Intel had kept Hamidi from using its servers, he would have no complaint that it had interfered with his liberty to speak to Intel's employees. At this point, why deny a legal remedy when the self-help remedy turns out to be inadequate? As Morrison, J., in the Court of Appeals had written below:

> Hamidi acknowledges Intel's right to self help and urges Intel could take further steps to fend off his e-mails. He has shown he will try to evade Intel's security. We conceive of no public benefit from this wasteful cat-and-mouse game which justifies depriving Intel of an injunction. . . . Even where a company cannot precisely measure the harm caused by an unwelcome intrusion, the fact the intrusion occurs supports a claim for trespass to chattels.[12]

This observation is right on the money. Frequently, the right to self-help is truncated because the legal remedy is supplied. But I am aware of *no* case in which the legal remedy is denied because the self-help remedy is available. The acceptance of self-help establishes that the owner of the chattel has an exclusive right to use it as he sees fit. If that cannot be defended unilaterally, then why should courts deny him standard legal regimes needed for its defense? Here Intel's losses from these trespasses (for such they are) are not trivial; for if they were, then why would Intel (and its industry supporters) have spent so much to protect its interests? These losses certainly count as consequential damages within the normal sense of tort law because the information was meant to upset the employees and did upset them. The use of the injunction is not meant to imply that Intel had no actual damages. Rather, its function was to obviate the costly procedures needed to prove damages with particularity in the hopes of obtaining long-lasting relief, which *did* work so long as the injunction remained in effect, without any collateral impact on the general operations on the Internet. On this score, Intel has simply followed the common practice in many contract cases: sue for specific performance of a contract of sale without asking for interim damages. The case doesn't begin to resemble pulling a dog's ears. The hoary precedents do not raise any issue that comes from using this chattel as a device for communication.

---

[12] Hamidi v. Intel Corp., 94 Cal. App. 4th 325, 332 (2001).

III. TRESPASS, NUISANCE AND LOW LEVEL HARMS

Part of the great theoretical interest in *Hamidi* stems from the range of tort doctrines that is relevant in choosing its final rule. To her credit, Justice Werdegar claims that cases of unauthorized server use are properly analogized to cases of low-level interference between neighbors, as in the ordinary nuisance cases. She writes as follows:

> Indeed, the metaphorical application of real property rules would not, by itself, transform a physically harmless electronic intrusion on a computer server into a trespass. That is because, under California law, intangible intrusions on land, including electromagnetic transmissions, are not actionable as trespasses (though they may be as nuisances) unless they cause physical damage to the real property. Since Intel does not claim Hamidi's electronically transmitted messages physically damaged its servers, it could not prove a trespass to land even were we to treat the computers as a type of real property. Some further extension of the conceit would be required, under which the electronic signals Hamidi sent would be recast as tangible intruders, perhaps as tiny messengers rushing through the "hallways" of Intel's computers and bursting out of employees' computers to read them Hamidi's missives. But such fictions promise more confusion than clarity in the law.[13]

In one sense this passage addresses the critical question of comparison and analogy. To Werdegar, the operative comparison is the rule that says that electromagnetic transmissions are physically harmless. That comparison should not be seen in isolation, but is part of a larger inquiry that deals with the full range of what might be called low-level interferences with the person or property of another person. For example, one could also ask the question about low level visual or aural stimuli that cause damage to extra sensitive individuals. Is there a tort if one person some distance away raises his hand to wave hello and second suffers severe emotional distress because he thinks that he is about to be assaulted? Is there an assault if people cannot bear to hear the sound of an ordinary human voice on the public street? Or shrink in horror when someone looks at them? The answer to these questions is a strong intuitive no. The hard question is not to defend that intuition. It is to explain why it is correct and why the *Hamidi* situation is totally distinct from it.

The best way to break down the analysis is to move from simple cases to complex ones. The simplest case of cybertrespass arises where one party sends a *single* electron into the space of another individual: I will put aside the question of whether it is to real or personal property for the moment. The initial principle that governs these cases starts with the assumption that the *inviolate* nature of property necessarily implies *any* entry into the land

---

[13] Intel Corp. v. Hamidi, 71 P.3d 296, 309 (Cal. 2003).

of another, no matter how minute, counts as a trespass, or a single particle of dirt sent by one landowner onto the property of another counts as a nuisance, i.e., an invasion of matter from one party to another.[14] Now, these accounts are intended to invite the protest that infringements so small could not count as wrongs at all. But that point is not quite responsive to the question, for the issue on the table is not whether there is an *actionable* trespass or nuisance, but whether there is any trespass or nuisance at all. In dealing with the question of actionability, the difficulties of demarcating the line between trespass and nuisance, which have occupied so much time in the case law[15] and the academic literature,[16] are beside the point. The first question one has to decide is what counts as a wrong, any wrong, at all.

If *any* invasion, however small, counts as a compromise of the exclusive right of possession, why should there ever be any *non*actionable trespasses? Here are two explanations, with somewhat different implications. The first of these is that the harm in question from a single particle of smoke or a single electron is simply de minimis, so that the law should not concern itself with trifles. This point is rarely litigated in the cases because it seldom makes any sense for anyone to pursue a legal remedy, even if costs are awarded, for damages so small. The expected return is still negative. It is for this reason that people do not sue because someone has touched their dog.

The argument, however, does not end here, for it is easy to identify a broad class of cases that promises gold at the end of the rainbow. Thus, envision a typical low-level nuisance in which the sounds of voices or machines make their way across the boundary line of two separate individuals. If any level of invasion counts as actionable, then the aggrieved party could seek not only damages, which are likely to be trivial, but also an injunction, which could prove to be much more potent if it threatens to stop a defendant from engaging in certain activities that produce high value on the one side, and only tiny losses on the other. The buyouts from multiple suits offer a transactional thicket with no social gain. It is for that reason that standard definitions of nuisance start with a threshold above de minimis, and require some unreasonable interference with the use and enjoyment of land.[17] It is not that the law commits itself to a negligence standard that

---

[14] The standard definition states that a private nuisance is "a nontrespassory invasion of another's interest in the private use and enjoyment of [his own] land." Restatement (Second) of Torts § 821D (1979).

[15] *See, e.g.*, Martin v. Reynolds Metals Co., 342 P.2d 790 (OR 1959) (treating released quantities of fluoride gas as a trespass, subject to a six-year statute of limitations, and not the two-year statute for nuisances). The distinction does not go to the wrongfulness of the conduct.

[16] Thomas Merrill, *Trespass, Nuisance, and the Costs of Determining Property Rights*, 14 J. LEGAL STUD. 13 (1985).

[17] *See, e.g.*, Cal. Civ. Code § 3479 (West 1997). The entire statute reads as follows:

> Anything which is injurious to health, including, but not limited to, the illegal sale of controlled substances, or is indecent or offensive to the senses, or an obstruction to the free use

balances costs and benefits before deciding what conduct counts as a nuisance, although there is surely authority that cuts in that direction.[18] Rather, for this purpose, the unreasonableness test only redefines the baseline above which nuisances are actionable. The de minimis stuff is out from the legal system even if a strict liability standard applies to more substantial wrongs. It is important to extirpate the socially destructive prospect of universal injunctive relief for ubiquitous trivial harms.

The justification for this position, however, does not rest solely on the minimal nature of the harm, but also on its reciprocal nature across multiple landowners. Low-level nuisances rarely run in one direction only. If my talking bothers you, then the sound of the baseball bat in your backyard bothers me. To avert the spectacle of lawsuits of all against all, the common law adopted a rule of "live-and-let-live."[19] The point here is that high transaction costs preclude any comprehensive voluntary release of rights to sue for low-level nuisances across the board. But a legal regime that knocks out all these actions between neighbors at once creates an overall social improvement from which all individuals share in roughly equal measure. It is as though an interest in property has been taken with one hand (i.e., the loss of the action for nuisance) for which just compensation has been supplied with the other (i.e., the release of actions from all others).[20]

This line of argument helps explain why low-level intangible intrusions on land, including electronic transmissions, do not count as trespasses or nuisances in the absence of real harm. Thus, to see why this rule is an absolute necessity, imagine what the world would look like in its absence. We should have a situation in which all broadcast (like all air transportation) would cease because each landowner could impose a blockade over all transmissions unless compensated for the entry. To avoid this problem, the

---

of property, so as to interfere with the comfortable enjoyment of life or property, or unlawfully obstructs the free passage or use, in the customary manner, of any navigable lake, or river, bay, stream, canal, or basin, or any public park, square, street, or highway, is a nuisance.

See also, Restatement (Second) of Torts: Unreasonableness of Intentional Invasion §826 (1979).

An intentional invasion of another's interest in the use and enjoyment of land is unreasonable if

(a) the gravity of the harm outweighs the utility of the actor's conduct, or

(b) the harm caused by the conduct is serious and the financial burden of compensating for this and similar harm to others would not make the continuation of the conduct not feasible.

For the alternative reading of unreasonableness that stresses only the level of the intrusion, and not the level of care, see *Jost v. Dairyland Power Coop.*, 172 N.W.2d 647, 650-652 (Wis. 1969).

[18] *See, e.g.* Copart Indus., Inc. v. Consol. Edison Co. of New York, Inc. 362 N.E.2d 968 (N.Y. 1977).

[19] For the decisive judicial elaboration, see *Bamford v. Turnley*, 122 Eng. Rep. 27 (Ex. Ch. 1862). For my discussion of the theme, see Richard A. Epstein, *Nuisance Law: Corrective Justice and Its Utilitarian Constraints*, 8 J. LEGAL STUD. 49, 74-79 (1979).

[20] Richard A. Epstein, TAKINGS: PRIVATE PROPERTY AND THE POWER OF EMINENT DOMAIN (1985).

law invokes a set of legally-imposed forced exchanges on the live-and-let-live principle. Everyone is forced to give up his blockade rights in exchange for the like surrender by others. Now all can receive transmissions that none can block. The normal rules of intrusion are relaxed across the entire property, not just some defined corridor, precisely because the propagation of waves moves in all directions simultaneously. The same argument, of course, applies to air traffic, only here there is a highway in the sky, which is organized and policed by the Federal Aviation Administration.

This basic rule is subject to a well-established exception that applies to both air transportation and electronic transmission. If the defendant's operation imposes a disproportionate burden on a single landowner or small group thereof, then some remedy (not necessarily an injunction) is allowed. Here the common cases with land are the airplane overflights needed to land and take off. But the remedy is not to deny an airplane the right to do either. Instead, it is to condemn the appropriate rights of way for just compensation. The parties who are specially aggrieved are now left as well off as everyone else.[21] The actual nuisance rule for electronic transmission works the same way: if your cows are injured by the transmission, then some relief is awarded.[22] Since these are particularistic injuries, the suit does not shut down the network. It requires only higher precautions, in the form of greater insulation, rerouting of wires, change in frequency or, since a public utility is involved, in the last instance, condemnation of the needed easement.

None, repeat none, of these issues are at stake in *Hamidi.* The proof lies in the nature of the remedial choices. *Hamidi* is a situation in which injunctive relief was banned, but self-help was *allowed* on the premise that property rights are inviolate. But the electronic transmission cases are governed by the exact opposite principles. The incursions here are all full-blown exceptions to the general rule on exclusivity, but they are exceptions that *flip over* the rights. It is not as though the live-let-live rules between ordinary neighbors allow either party to use self-help to block the activities of the other. The rule in effect gives each side reciprocal *easements* over the property of the other, and, with the property rights redefined, that easement can be protected both by self-help, damages, and injunctive relief. The same rule applies to electromagnetic transmissions for broadcast. The rule is not that a landowner may use tin foil (or any more modern device) to

---

[21] *See* Neiswonger v. Goodyear Tire & Rubber Co., 35 F.2d 761 (N.D. Ohio 1929) (treating low level intrusions, below 500 feet as trespasses, while recognizing the high level overflights are not). This rule necessarily infringes the old common law rule that extends property rights to the ends of the heavens. It is pointless to deny the infringement, but decisive to point to the enormous benefits that all landowners gain from the mutual relaxation of these restrictions. For discussion, see TAKINGS, *supra* at 49-51, 234-236.

[22] *See, e.g.* Vogel v. Grant-Lafayette Elec. Coop., 548 N.W.2d 829 (Wis. 1996).

block the transmission. It is that a new property right (fully justified by the benefits it generates) precludes any interference at all from landowners below, even as it allows one broadcaster to enjoin interference from a rival broadcaster operating on a nearby frequency.

Note the implicit logic of the nuisance cases. The property rights in land are redefined precisely because the allocative consequences are positive, and the implicit level of redistribution when all is said and done is zero. In its most general form the proposition is this: In the ordinary situation we start with universal rights of exclusion as the *first* approximation to an optimal division of property rights. But at no point is the allegiance to that definition so unswerving that it precludes a search for Pareto improvements, which can be found by the mutual toleration of low-level interferences. In this case, moreover, it is clear that the division of gains is not likely to be skewed in favor of any particular group, which makes the change even more desirable.

In Henry Smith's terms, it is not as though we create a complex governance structure to decide which uses of real estate are appropriate and which not. Rather, in the live-and-let-live cases, we allow for limited crafted exceptions (that are themselves rules) to the general rules of exclusion. These exceptions meet the strict Paretian tests, which require us to make judgments along only a single dimension: the magnitude of the intrusion.[23] Far from having a muddy nuisance law, this regime is consistent with a rule that normally allows an injunction as of right against any party that has committed a private intrusion on a continuous basis.[24] The last thing that is needed is an approach that asks courts to adjudicate which kinds of intrusion should be allowed, and which should be kept off. In this regard, Professor Burk's highly influential article is wide of the mark when it says: "The 'muddy' nature of nuisance would allow computer owners on the net to exclude unreasonably costly uses of their servers, while allowing socially beneficial uses, even if the server owner might otherwise object."[25] When applied to the content of particular messages, which is what is at stake here, this approach, which is said to serve First Amendment interests,[26] in reality runs against it. The last thing that we need is for the state to decide which forms of speech are beneficial enough to justify a trespass

---

[23] Henry E. Smith, *Self-Help and the Nature of Property*, 1 J.L. ECON. & POL'Y (2005); and his piece in the Yale Journal of Regulation. (forthcoming) Check itation with Smith

[24] The one case that modifies this rule, *Boomer v. Atl. Cement Co.*, 257 N.E.2d 870 (N.Y. 1970), tends to apply only in a few cases. The older, and sounder, rule blocks the nuisance and drives the process back into the public processes of the eminent domain law. *See, e.g.* Whalen v. Union Bag & Paper Co. 101 N.E. 805 (N.Y. 1913) (where the injunction was allowed for the benefit of a lower riparian whose losses were small on the ground that the balancing of the equities was not in order). Note that such discretion normally is allowed in the timing of relief, so that the defendant is given some time to reorient his business, at least in the absence of imminent peril.

[25] Dan Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53 (2000).

[26] *Id.* at 52-53.

action and which are not. No court has the institutional competence to make that kind of judgment over the full range of cases, which accounts for the high-level of suspicion that is brought to content-based distinctions, especially on matters of viewpoint, in virtually all First Amendment contexts.[27] No one would argue that a person is under a duty to open his home or business to some kinds of speech but not others. It hardly makes a difference that Hamidi wants to enter Intel's business by Internet or on foot. The unauthorized entry has long been regarded as a per se violation under ordinary trespass principles. There is no reason to back off that view here.

The same type of argument is made with various forms of subjective personal affronts that take place in various settings. When a student, for example, enters a classroom he cannot complain if the ordinary voices cause him acute mental distress. The rule here is that ordinary conversation means that the baseline on matters of sound is not zero, but is set high enough to allow for ordinary communication to take place. When people talk on the public street, or over the backyard fence, the same rule of live-and-let-live applies as well. Everyone gives up a tiny bit of personal autonomy in exchange for the far greater freedom of action that is allowed from the universal relaxation of the strict autonomy rule. But once again, the principle is subject to limitations analogous to those used for takeoffs and landings. Loud sounds disrupt public peace and quiet; bright lights cause physical distress; staring or stalking people on the public way creates uneasiness. These higher level actions are not allowed because a one-sided shift in the balance of advantage precludes a Pareto improvement. The gains from these invasions of individual autonomy are tiny, and the dislocations are great. What are left are hard cases in the middle: The church rings a bell that sounds loud to a sick person who lives nearby but is enjoyed by others.[28] The law of nuisance, in a close decision, refuses to allow the action even for serious physical harms. The baseline for large social phenomenon is not taken to be the position of the extrasensitive individual, but of the ordinary citizen.

The systematic effects could not be more different in the *Hamidi* situation, where none of these elements of reciprocal forbearance play the slightest role. No one claims that Hamidi has strong property rights that preclude Intel's use of self-help. Here the plaintiff seeking damages is not in the position of someone that prevents the use of the atmosphere as a source of communication. Rather, the case here is one in which the defendant is making an unauthorized use of the plaintiff's property for which there is not the slightest element of reciprocity or compensation. Stopping Hamidi, in a word, does nothing to disrupt the operation of any network, which is of course what is at stake in the cases of transmission of power or

---

[27] *See, e.g.*, Geoffrey R. Stone, *Content Regulation and the First Amendment*, 25 Wm. & Mary L. Rev. 189 (1983).

[28] Rogers v. Elliot, 15 N.E. 768 (Mass. 1888).

electromagnetic radiation. Hamidi, and everyone else, remains free to use the Internet. The only question is who gets to control the use of Intel's server.

Werdegar, J., misses the strong structural differentiation when she draws a collection of misguided analogies which claim that Hamidi "no more invaded Intel's property than does a protester holding a sign or shouting through a bullhorn outside corporate headquarters, posting a letter through the mail or telephoning to complain of a corporate practice."[29] But take these cases in order. The complaint here is not of the posting on the web or the shouting outside. No one denies that he can build and promote his web site or stream information to the homes of individual employees, subject of course to their individual consent. Rather, the analogy is a situation in which Hamidi uses Intel's bullhorn to project his own message. Werdegar's description of the parallel ignores the element of unauthorized use. Posting a letter through the mail cuts in the opposite direction. It is well established that any addressee can refuse to accept the mail, or even request the United States Post Office not to deliver it. So long as the choice is made by the addressee and not the government, the issues of censorship do not apply, and the prohibition is allowed precisely to prevent the harm that Hamidi is causing. They can keep that mail out of their own box for whatever reason they choose, including keeping it out of the hands of employees who might become distressed or distracted. The right of self-help is not limited because of employee interests; the injunctive relief should not be limited either.[30] Similarly, the state cannot, under the First Amendment, impose a general restriction on the ability of canvassers to enter the land of ordinary residents, but that does not preclude a landowner from posting a "no-solicitation" sign that all outsiders are bound to respect.[31]

Next, the telephone call becomes a wrong if done after an explicit instruction not to do it again, which is why the Do Not Call Registries have proved to be a runaway success.[32] The reason we establish do-not-call registries is that normal people don't bring lawsuits because of the occasional disruption, which is hardly reason to deny someone who has suffered major losses from bringing the suit. And here the question of magnitude matters. The analogy to Intel is not the isolated phone call: it is whether a company could protest if a hacker broke into its exchange and sent the same auto-

---

29 *Hamidi*, 71 P.3d at 312.

30 Rowan v. United States Post Office Department, 397 U.S. 728 (1970).

31 Martin v. Struthers, 319 U.S. 141 (1943); *see also* Watchtower Bible and Tract Society of New York v. Village of Stratton, 536 U.S. 150 (2002), which struck down a similar municipal ordinance while noting that insofar as the law "it seems clear that § 107 of the ordinance, which provides for the posting of "No Solicitation" signs and which is not challenged in this case, coupled with the resident's unquestioned right to refuse to engage in conversation with unwelcome visitors, provides ample protection for the unwilling listener." *Id.* at 168.

32 D. Reed Freeman Jr., *Do Not Call List is not the Only Victor*, 20 E-Commerce L. & Strategy, (No. 7) 1 (2003).

mated telephone message by machine simultaneously to 35,000 people. The doctrine of implied consent that works for the first call does not continue to work indefinitely no matter how great the intrusion. So long as self-help is allowed to stop the conduct, why block the legal remedy for those who have made the unwillingness to talk clear?

IV. METAPHORS AND ANALOGIES: FROM REAL TO CYBERSPACE

The general discussion of nuisance and trespass law shows that it is wrong to think that the unauthorized use of someone else's equipment should be treated like overflights or electronic transmissions. Indeed, those insights go further in the argument. When *Hamidi* was before the California Supreme Court, my own amicus contribution to this debate was to rethink whether the hoary rules of trespass to chattels should apply to this dispute in light of the functional differences between a dog's ear and the Internet. My brief started with the elementary proposition that the Internet is a network industry.[33] As such, it resembles another network, public highways, which offer open access to the private homes and businesses adjacent to them. Anyone from one private plot of land can use the highway to reach anyone else adjacent to the highway. Perfect connectivity holds between and among all private sites along all public roads. The two forms of property, private and common, work together to produce outputs that are far higher than could be achieved by any legal regime that might be foolish enough to opt for either form of property rights alone.

How does this play out for the rules of trespass to Intel's server? Here the key clue comes from the alternative term used to describe chattels: movables. The reason why we do not award damages for trivial losses to dogs and chairs is that their owner can easily move them out of harm's way. But there is no way to achieve that objective with an on-line computer. Move it from the office to the home, and it will still be on-line. The only way to get out of harm's way is to log off the central system. In this regard, the private Internet sites along the Internet highway function just like ordinary homes and businesses, which also cannot be moved out of harm's way. If the functions run in parallel, then the legal rules should run in parallel as well. Hence, the keep off sign is respected wholly without regard to actionable damages.

Now there are a variety of objections that could be raised to this argument, the first of which is terminological. Werdegar, J., writes as follows:

> Epstein's argument derives, in part, from the familiar metaphor of the Internet as a physical space, reflected in much of the language that has been used to describe it: "cyberspace," "the information superhighway," e-mail "addresses," and the like. Of course, the Internet is also

33 *See*, OZ SHY, THE ECONOMICS OF NETWORK INDUSTRIES 1-6 (2001).

> frequently called simply the "Net," a term, Hamidi points out, "evoking a fisherman's chattel." A major component of the Internet is the World Wide ""Web," a descriptive term suggesting neither personal nor real property, and "cyberspace" itself has come to be known by the oxymoronic phrase "virtual reality," which would suggest that any real property "located" in "cyberspace" must be "virtually real" property. Metaphor is a two-edged sword.[34]

Justice Werdegar's fanciful use of etymology to break the parallel between physical and cyberspace is totally misguided. In one of the worst plays on words imaginable, she concocts a derivation for the term Internet that is false to its history and understanding. The word Internet derives from inter-network, which morphed into inter-net, which evolved to become Internet. The use of the term "web" gains its power *precisely* because the web involves the intricate network of fibers that exhibit connectivity even if used for some different purpose. If anything, the origin of the term "net," as in fisherman's net, (which we can safely concede is a chattel) runs in the opposite direction. A net looks like a network because of the connections between its various nodes. The simple description of the Internet follows and conforms to the most rigorous definition of a network industry, which include telephones, email, Internet, airlines and railroads.[35] The standard economic analysis runs the same for all these networks notwithstanding that they operate in different forms of space. The connection that is seamlessly made in economics can and should be made as well in law.

Part of the reason why Judge Werdegar goes so far astray is that she has been badly misled by the use of a metaphor that has been the darling of recent commentators[36] to debunk Intel's claim by arguing that any effort to think of cyberspace as a "place" suffers the grievous sin of physicality. This inapt metaphor leads to unsound thinking about property rights in cyberspace. The most detailed treatment of this topic is from Dan Hunter who exhaustively demonstrates a point that no one on any side of the debate should care to contest: namely, much of law consists of a battle to choose the right metaphor to govern a particular situation.[37] The key issue on the use of metaphor, which Hunter nowhere addresses, is why do some metaphors succeed when others fail? Hunter demonstrates in an impressive number of cases the tenacity with which metaphors entrench themselves in ordinary language. Charges and defenses, parries and thrust are the business of war, where the terms have a definite physical referent. Law, and other forms of argument, often involve verbal clashes (another metaphor?) between individuals whose desires and ambitions are inconsistent with each other. A plaintiff with a weak case faces an uphill battle precisely because

---

34 *Hamidi*, at 309. .

35 Oz Shy, The Economics of Network Industries 1 (2001).

36 *See* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 Cal. L. Rev. 439 (2003), Lemley, *supra* note 8; *See contra*, David McGowan, *The Trespass Trouble and the Metaphor Muddle*, 1 J.L. ECON. & POL'Y (2005).

37 Hunter, *supra* note 36.

it is harder to attack from below than from above (which is why ordinary people kneel before potentates who sit on thrones). But no one thinks that gravity is the source of the difficulty in verbal or written argument even if it plays an insistent if silent role in all physical situations.

Stated simply, these physical metaphors stick over time precisely because they are found time and again in ordinary conversation to be accurate reflections of the new state of affairs. Those metaphors that don't will fail. For example, in his commentary on Hunter, Mark Lemley invokes a water metaphor for internet trespass cases as "chasing down electronic 'water' in order to reclaim it."[38] But we can be confident that this metaphor will fall stillborn from the press. And for good reason. The comparison is flawed because rivers and lakes have multiple in-stream and consumptive uses that go beyond transportation. The description of an internet highway captures the single nature of the use of the common resource that the water metaphor misses. All this is not to say that water metaphors never work. When people talk about controlling their "flow" of work, it is no longer a metaphor. The constant movement of small tasks across the desk does evoke the image of water. No one is misled because work flow is not wet. So it is that the highway metaphor sticks in cyberspace because it offers an accurate analogy to a familiar state of affairs. In time what starts as metaphor insensibly becomes description. That transformation, it must be stressed, is not the work of a single iconoclastic individual. The metaphors take grip because they allow everyone to communicate with greater ease than is possible with elaborate circumlocutions that are devoid of physical referent. If there were ever a case where the Hayekian views of decentralized, spontaneous evolution work well, it is in the development of language, where even the French cannot resist the popular bottom up sentiment.

It is just this process that led to the development of the rich and stable vocabulary on sites, places and spaces that everyone uses to describe life on the Internet. Indeed, to constantly remind individuals that the Internet is composed of electrons that follow certain protocols is to ordinary individuals the use of stilted language. (Quick: why does this "metaphor" work?) The point is relevant to the whole *Hamidi* dispute. Thus beware when Mark Lemley uses the double quotation marks to deconstruct ordinary English when he writes: "They [courts] have not understood that no one 'enters' websites. Rather, the defendants in these cases merely sent requests to a web server that the plaintiff opened up to the public, and the plaintiff's server sent information in return."[39] Of course, courts understand the architecture. Anyone who wants to stress how communications between computers technically work might be concerned with these protocols. But people who want to know whether the communication took place are quite

---

[38] Lemley, supra note 8, at 538. For his awareness of the weaknesses of his own suggestion, *see id.*

[39] Lemley, *supra* note 8, at 528

happy to *describe* the defendant as entering the plaintiff's space, as indeed even Hunter and Lemley would have to concede if they were to conceive of these cases, including spam, as trespass to chattels, all of which require entry. What has happened in the use of the quotation marks is an effort to breakdown the dominant paradigm that ordinary people use to understand these cases. It is exactly the same strategy that courts and commentators used to deconstruct the word "nuisance" in the takings cases, here in order to undermine any of the traditional limitations of the state's police power.[40] That difficulty is in turn compounded by smuggling into the proposition that somehow these sites were "open to the public," as if that false description somehow precluded the right of any site owner to exclude anyone from the site.

The blunt truth is that the effort to use semantic arguments to displace the standard language used to describe cyberspace falls of its own weight. The hard question is whether the metaphorical skeptics are able to demonstrate inefficient or adverse social consequences that follow from its adoption. Here Werdegar, J., takes her lead from Mark Lemley and Lawrence Lessig, now both of the Stanford Law School:

> Other scholars are less optimistic about such a complete propertization of the Internet. Professor Mark Lemley of the University of California, Berkeley, writing on behalf of an amici curiae group of professors of intellectual property and computer law, observes that under a property rule of server inviolability, "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel." The consequence for e-mail could be a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source. . . . A leading scholar of Internet law and policy, Professor Lawrence Lessig of Stanford University, has criticized Professor Epstein's theory of the computer server as quasi-real property, previously put forward in the eBay case, on the ground that it ignores the costs to society in the loss of network benefits: "eBay benefits

---

[40] For an illustration of the practice, see Frank I. Michelman, *Property, Utility, and Fairness: Comments on the Ethical Foundations of "Just Compensation" Law*, 80 Harv. L. Rev. 1165, 1196-1211 (1967) in which quotations are put around the words "harms", "benefits,", "neutral," "nuisance prevention," "smoke nuisance," and "antinuisance," "nuisance" "the better," "intolerable harm," "wrong," "the public," and "public," and in the footnotes, "fault," and "noxious use." The quotation marks are not used to indicate cited material, but to show the uneasiness that Michelman feels towards the traditional categories of analysis that under gird a stronger reader of the takings clause. For judicial efforts along the same line, *see* Miller v. Schoene, 276 U.S. 272 (1928), *discussed by* Michelman, *id.* at 1198-1199. In *Miller* the court sustained a Virginia statute that allowed cutting down of cedar treats, without compensation, that harbored a dangerous pest in order to save the more valuable apple trees from destruction. The Court did not rely on the control of infection as a justification for the action. Indeed, it ran away from the nuisance language altogether: "We need not weigh with nicety the question whether the infected cedars constitute a nuisance according to the common law; or whether they may be so declared by statute. For where, as here, the choice is unavoidable, we cannot say that its exercise, controlled by considerations of social policy which are not unreasonable, involves any denial of due process." *Id.* at 280. It is ironic in the takings context the effort is to trash the traditional law of nuisance because of its vagueness, while in the cyberspace context the critics of Intel's position work, like Burk, to make nuisance the paradigm.

> greatly from a network that is open and where access is free. It is this general feature of the Net that makes the Net so valuable to users and a source of great innovation. And to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines. If machines must negotiate before entering any individual site, then the costs of using the network climb." (Lessig, The Future of Ideas: The Fate of the Commons in a Connected World (2001) p. 171)[41]

The confusions contained in this short passage are legion. First, the proposal to treat web sites as real property is not intended to work a complete "propertization" of the Internet. It is only to have the same distribution between private and common property rights that is observed within the physical universe for the parallel problems of insuring general connectivity and private investment. On this regard, Lemley's article on Place and Cyberspace contains a long discussion about the necessity to have common as well as private property in ordinary space.[42] He notes that even in the physical world it would be ludicrous to treat private property as the exclusive regime. Thus, he rightly notes it would be wholly mistaken to assume that the physical world is devoid of public parks, libraries, and museums. And he recognizes the critical role that social infrastructure plays in allowing individuals to move from one plot of private land to another by rail, road, river and air. Further, he rightly stresses that the inconvenience of private roads would be great if individuals were required to pay tolls whenever they crossed in front of the land of private individuals—in yet another stark reminder of the hold that the anticommons now has over us all.

But he never connects the dots. Those of us who favor the extension of the trespass to land rules to the Internet do not disparage the place of public property in any of the senses to which Lemley refers. It is quite permissible to set up an on-line museum or library that all the public can enter at their free will and pleasure—even if we impose a do not disturb sign on the exhibits that they see. Likewise, it is necessary to create and maintain the social infrastructure in cyberspace as in physical space. But what Lemley does not explain is why this summary of the ordinary division of physical space does not carry over to cyberspace in allowing for some private property on the Internet. His disquisition on the public nature of the space appears to preclude the use of self-help for the protection of chattels. Yet once again, the standard legal doctrine to which he appeals concedes that the chattel is private property, and inviolate at that.

What makes it still more ironic is that the precise division of common and private property underlay my critique of Hamidi's distinction. In seeking an optimal mix of common and private property, I pointed to the basic tension that is pervasive throughout property law that carries over to cyber-

---

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

42 Lemley, *supra* note 8, at 533-43.

space without missing a beat.[43] A sound system of property law has to provide the owner of any resource with the knowledge that he will be able to appropriate the return on his investment, which is captured by the agricultural metaphor: that he who sows shall reap.[44] But at the same time, the rules in question must also be concerned about the problem of coordination among separate owners when cooperation is necessary to realize the value of their resources, in what has come to be called the anticommons problem. There are two key points here. First, anything that tends to strengthen the individual right to exclude will make coordination more difficult. But the creation of any commons will chill the incentive to invest. Second, there is no way to be perfect on both these margins simultaneously, so that the optimal choice of any legal system will be dependent on the nature of the resource in question. The use of the model of exclusion for water is, for example, a most unfortunate starting place because the problems of running water make the coordination question the first order of business, to which corrections can be made to allow for private uses.[45]

With this said, the challenge still remains: where is the inefficiency in applying the model of trespass to real property for web sites along the Internet highway? Lemley tries to meet that challenge by noting that the highways in cyberspace work much more rapidly and anonymously than those in physical space.[46] But there is no explanation of why speed matters. The division between public and private roads did not disappear when we moved from horse drawn carriages to automobiles. To be sure, in physical space, the change in speed and the frequency of traffic carries with it the risk of greater noise damage which is not a problem in cyberspace. But that difference only means that the Internet highway can operate more efficiently because it generates fewer negative externalities on neighbors. The conclusion is that Internet designers do not have to build large barriers to muffle the sound of the sort often found when main arteries (another metaphor turned description) run through populated areas. This factual truth hardly explains why the rules that adjust the boundary conditions between web sites and the Internet highway have to change because the Internet offers the better transportation.

---

[43] Richard A. Epstein, *On the Optimal Mix of Common and Private Property*, 11 Soc. Phil. & Pol. (No. 2) 17 (1994).

[44] Which was introduced with great effort to deal with the tort of misappropriation of information, before cyberspace. *See International News Service v. Associated Press*, 248 U.S. 215 (1918). *For discussion, see* Douglas G. Baird, *Information, Uncertainty, and the Transfer of Property*, 13 J. Legal Stud. 299 (1984); Richard A. Epstein, *International News Service v. Associated Press: Custom and Law As Sources of Property Rights in News*, 78 Va. L. Rev. 85 (1992).

[45] I am told that there is an exception for small streams in Scotland that are entirely contained on large estates. At this point, there is no reason to worry about the coordination among multiple riparians and other users, so that the standard exclusivity models can apply.

[46] Lemley, *supra* note 8, at 527.

Lemley also claims that transactions on private land are observable from highways. In talking about the famous case of *eBay v. Bidder's Edge, Inc.*,[47] Lemley claims that any one who is kicked out of a private auction house can observe from the street which buyer has taken home a chesterfield, and then share that information with others.[48] But that is just not so. The owner of the house may have a back entrance through which the buyer could disappear. Or he could crate the purchase in a box so that an outsider could not observe it. Indeed, in live auctions, it is common for customers to bid by telephone, or to use hand signals, or to bid through proxies, in order to keep their identity concealed from other bidders. It hardly counts as a reason to reverse the law of trespass that legitimate ends could be achieved in cyberspace at lower cost. Lemley and others object to this conclusion on the ground that all information has positive value so that no one should be excluded by its nonrivalrous use. But this view of information ignores the fact that Hamidi was not sending pages from the almanac or the financials. These messages were not information with any positive value for the recipient, and Hamidi knew that. At this point the great advantage of a system of private property is that it allows each person to decide for himself whether certain material counts as information or disinformation. The issue here parallels that with the general preference for property regimes in the absence of cases of strong necessity. A voluntary license from a clear distribution of rights will outperform any system of coerced licenses, which

---

[47] 100 F. Supp. 2d 1058 (N.D. Cal. 2000). For the record, I wrote an amicus brief for eBay against Bidder's Edge, which is now out of business after it abandoned its appeal. At issue in that case was whether an "auction aggregator" was able to send "spiders" through eBay's sites to collect information about the prices of various goods on sale. The court granted eBay and injunction against the activity. Note that the eBay case raises different issues from *Hamidi* in that there no one claimed that the information was a source of distress. The case did raise questions of whether eBay should be able to protect the information it assembled from rival bidders who were prepared (as Bidder's Edge was not) to enter into agreements that would allow cooperation between firms. Note too that behind *eBay v. Bidder's Edge* was the possibility of an antitrust suit on the grounds that eBay, even though it was acting alone, had engaged in monopolization of the relevant market. I am deeply suspicious of all section 2 claims, see Richard A. Epstein, Monopoly Dominance or Level Playing Field: The New Antitrust Paradox, 72 U. Chi. L. Rev. 49 (2005). But even if these are valid, there is no reason to use the possibility of this claim to the law of trespass from its ideal.

eBay sued Bidder's Edge (BE) for trespass to chattels. BE was an auction aggregator who sought to give its customers the ability to compare prices for items that were sold on different sites. To obtain the needed information, BE used its Internet "spiders" to search eBay's online auction database thousands of times per hour, in order to post auction updates on its own website. Although eBay's database was publicly accessible, its stated policies forbade anyone from probing its space with spiders. When BE refused to discontinue its "spidering," the court granted eBay a preliminary injunction against BE's activities, finding that these recursive searches amounted to trespass to chattels, capable of impairing the operation of its site.

[48] Lemley, *supra* note 8, at 536.

cannot be sensitive to the differences in local environments.[49] There is no reason to have any collective decisions on the question of entry, which is yet another reason why the strong injunctive remedy should apply. It is for just this reason that the lower court was right to rely on physical metaphors drawn from a brick and mortar world.[50]

In making these comparisons and analogies, it is absolutely critical to make sure that the rules are accurately stated in both domains. Thus, with *Hamidi*, this point is of exceptional importance in dealing with the issues of express and implied consent to enter someone else's web site. More concretely, the creation of a system of strong protection for individual internet sites carries with it the implication that no one is allowed to call on the Internet without receiving permission in advance from those who own servers through which their message travels. What applies here is the same convention that has long governed the use of the telephone. We have and need a doctrine of *implied* consent, sanctioned by long social convention, to ease communications. You may call anyone *once* without permission. But once he has told you in no uncertain terms not to call again, then it is a trespass to call again, which could lead to an injunction if the caller continues to pester. In *Hamidi*, moreover, the stakes are much higher because the unwanted communications are made to hundreds of separate individuals who are within the private network within the firm. All that is asked is that people who are told to stay off your site respect your wishes.

Nor are there any deep fears that should be addressed. The injunction that Intel had received from the trial judge remained in effect for about three years and it produced none of the dreadful consequences of requiring routine permission in advance that either Lemley or Lessig predicted. Quite the opposite. The level of communication on the Internet is likely to increase if individuals who link up to the web know that they have the power to keep out unwanted communications not only by self-help but also by legal assistance. The principles at work here are the same that govern a large store on a public road. The right to exclude gives the owner the benefit of traffic he wants, without having to incur the costs of traffic that he does not want. No one has to pay the price of admitting everyone in order to admit someone.

---

[49] *See, generally*, Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 Cal. L. Rev. 1293 (1996), noting that in the copyright area, the firms themselves were able to design a distinctive licensing system that was superior to any that the state could impose of its own will. For my discussion in connection with patents, *see* Richard A. Epstein, *Steady the Course: Property Rights in Genetic Material*, at 159, *in* 50 PERSPECTIVES ON PROPERTIES OF THE HUMAN GENOME PROJECT: ADVANCES IN GENETICS (F. Scott Kieff, ed., 2003).

[50] "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. . . ." *eBay*, 100 F. Supp. 2d at 1067. Note that this court sees, rightly, that if self-help does not work, then a legal remedy should apply.

V. FROM *HAMIDI* TO SPAM

To all these objections, it might be asked, what difference does the decision in *Hamidi* make? The intellectual consequences are that it leads to a misunderstanding of the way in which a sound property system is organized. This misunderstanding 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. But for these purposes, I will not dwell on the long-term implications that *Hamidi* could have if its influence spreads into the law of intellectual or real property, but will instead concentrate on an issue close to this Conference: spam. My fear is that *Hamidi* will complicate the fight against the various forms of spam. Here there are two issues that have to be faced. The first is the question of whether a doctrine of implied consent should in principle protect a spammer who can always claim that his conduct is done with an eye to providing benefits to the recipient. The second issue is what responses should be taken against spam once the doctrine of implied consent is confined to manageable proportions.

Regarding the first, the question is difficult because, after all, some fraction of these offers is accepted. That issue will not just disappear, but it seems clear that we should aspire to create some mechanism to allow ordinary users of the Internet not to receive these mass e-mailings. A simple list, like the do-not-call registry, might be a good place to start. "I do not wish to receive any message from any person with whom I have no relations, if it is sent, directly or indirectly, to more than 1000 people." But this task is not easy, as the limited effectiveness of the CAN-SPAM Act reminds us. At a minimum, further rules may be needed to deal with membership organizations and the like, but it should be doable. Additional rules might be appropriate for the 200 most infamous spammers, who could be presumptively excluded (along with their affiliated organizations) unless explicitly allowed. It is easy to multiply the complications, but it should be possible to do something useful—at least if injunctions against people and organizations are allowed.

Unfortunately, the ability to deal with spam can only be complicated by a decision like *Hamidi*, which does not see the harm in the unauthorized use of someone else's equipment as a wrong, and which systematically underestimates the importance of the network issues that the case raises. The going definition of spam concentrates on the use of bulk unsolicited mailings. As a first approximation what *Hamidi* sent was spam because it fits that definition. In truth, the fit is far from comfortable because Hamidi did not send the information to initiate some kind of a commercial transaction with a random slice of the population. His motives were much more focused, which in the eyes of some might make his actions more noble, but in the eyes of others make it a greater nuisance and danger. But once the law posits a situation in which some unauthorized uses are permissible and oth-

ers are not, then it has to draw a remedial line that need not be created under the rule that says that any presumption of free access is conclusively rebutted by clear notice from the owner to stay off.

Just how should that line be drawn in the standard spam situations? Thus, consider these two variations. First, suppose that we have a world with 1000 individuals who send out 100 million messages each day, but each of them sends only one email message to each person. Looked at from the point of view of *Hamidi*, there is no spam problem here. No one can claim that one message per day clogs the machine or taxes the individuals who receive it. And the spammer could say that he is being singled out because of the content of his message. But when all 1000 spammers are taken into account, the picture looks graver because 1000 messages per day undercut the effectiveness of the system in multiple ways. They clog the traffic on the web and they clog the machines of the individuals to whom they are sent. The question is whether decisions like *Hamidi* limit the defense to self-help. If so, does the case still bite, if the pattern of messages shifts so that each spammer now sends 100 messages each day to one million persons? The ultimate volume of traffic sent and received is precisely as it was in the first case, so why think that a remedy should be allowed here but not in the first instance. The key point is that all that matters from a network perspective is the total volume that is sent out; the question of who receives each individual message is neither here nor there. *Hamidi* places one more gratuitous obstacle in the path of gaining some protection against spam, which is already difficult because of the need for a coordinated attack.

Here is another problem, which was brought to my attention by my colleague Randal Picker: zombies. These are machines that are quickly taken over by the master spammers and used to spit out vast quantities of messages in the background to all sorts of people. They do not clog up the individual machine, but take advantage of the excess capacity that is built into so many modern machines. For just this reason, no one will take the individual steps, which can prove costly, to slay the zombie within. The price structure of broadband charges a fixed fee for all that one can send, so that there are no price effects adverse to the party whose machine is taken over. Perhaps all pricing rules should become volume responsive to counter that risk. But whether they do or do not, does anyone want to say that the use of zombies is not an actionable form of trespass? To be sure, *Hamidi* is distinguishable because it was directed at the employees of the plaintiff and not to third parties. And I suspect that actions for injunction would succeed at common law, whether brought on a class action basis or by way of government action. But why take the chance that the entire enterprise will misfire on this dimension? In this context, there is little wrong with the per se rule that says whenever self-help is allowed, then the injunctive relief may follow to the same effect. There was no sign of any dislocation in the use of the Internet while the *Hamidi* injunction was in place.

And there is a self-correcting mechanism that is at stake here that weeds out suits brought for little or no purpose. The problem with self-help in the context of network industries is not that it is likely to prove abusive, but that it is likely to prove insufficient. The tragedy of the *Hamidi* decision is that it failed to understand the systematic implications of that decision. It posited disruption of the network where none takes place. Yet, it ironically creates an obstacle of uncertain size in the effort to police the network externalities associated with spam.

VI. NEXT EPISODE?

There is, however, perhaps some light at the end of this tunnel. At present there exists a complex interaction between the law of free speech and the law of takings, which has as its hallmark the exclusivity point mentioned earlier. This point is the keystone of such significant decisions as *Kaiser Aetna v. United States*,[51] and *Loretto v. Teleprompter Manhattan CATV Corp.*,[52] both of which stress the importance of the right to exclude under the takings law. These cases hold the delicious prospect that the modest expansion of the law of trespass to chattels that was resisted in *Hamidi* could be reversed by turning this case into a federal constitutional challenge of a judicial taking of private property. If that happens, we shall add another chapter to the continuous dialogue over the rights and limits of private property, which will help bring the field back into equilibrium.

In dealing with the twists and turns of this subject, the long history of the self-help remedy shows both continuity and novelty when it applies to the law of cyberspace. In its original formation, self-help was the only remedy available, and its partial success depended on the ability of individuals to internalize the difference between aggression and defense and to act in accordance with that distinction. In a more complex legal system, self-help is still critical because there are many cases in which the legal system offers too little, comes too late or is too expensive. Yet there is no doubt that the availability of legal remedies in this context reduces some of the pressure on self-help, and channels many potential conflicts into more sensible modes of dispute resolution.

These principles apply with full force to the Internet. In cyberspace, the problems of coordination and abuse are paramount since all individuals are part of a single network. The best way to handle this problem is to adopt in cyberspace the same approach for defining the mix between common and private property. The latter is often the dominant form because it encourages investment. But when networks are at issue, the strong protection of property rights can create immense coordination problems that can-

---

51 444 U.S. 164 (1979).

52 458 U.S. 419 (1982).

not be reversed by contrary agreement. In these cases, property rights flip over so that all individuals get access to a network that no single person can block, similar to airwaves and aviation. Within cyberspace, there is no reason for network coordination to deny any owner of a site the right to exclude persons from access or use of its own facilities, so long as they have full access to the network system, because there is no equivalent of the broadcast or aviation blockade. That point was lost in *Hamidi*, with the odd consequence that the weak protection of private sites beside the Internet highway could have adverse consequences on the ability to keep that network open and available to all.

HACKING, POACHING, AND COUNTERATTACKING: DIGITAL COUNTERSTRIKES AND THE CONTOURS OF SELF-HELP

Bruce P. Smith[*]

For better or worse, self-help is alive and well in the realm of computer security. Of the nearly 500 American corporations, governmental agencies, financial entities, and academic institutions polled in the *2004 CSI/FBI Computer Crime and Security Survey*, virtually all employed antivirus software (99%) and firewalls (98%). Over 80% conducted security audits to identify network-related vulnerabilities. A substantial number participated in collaborative information-sharing organizations designed to collect and disseminate intelligence relating to online threats. And when these defensive measures failed and computer security incidents occurred, as they frequently did, over 90% of the respondents patched their security holes themselves.[1]

Given the challenges associated with ensuring optimal investment in network security – including "free rider" problems, barriers to information sharing, and sheer indifference – such levels of institutional commitment to network defense might appear, at first blush, to furnish grounds for optimism.[2] Yet a closer examination of the data compiled by the Computer

---

* Richard W. and Marie L. Corman Fellow; Co-Director, Illinois Legal History Program; Associate Professor of Law, University of Illinois College of Law. I am grateful to the editors of *The Journal of Law, Economics & Policy* for inviting me to participate in the symposium on "Property Rights on the Frontier: The Economics of Self-Help and Self-Defense in Cyberspace," to the *Journal* and the Critical Infrastructure Protection Project (CIPP) for sponsoring the proceedings, and to the symposium's attendees (especially Richard Epstein and Emily Frye) for their valuable comments. I have also benefited from the suggestions of Tom Ginsburg, Pat Keenan, Jay Kesan, Richard McAdams, Elizabeth Robischon, and Dan Vander Ploeg.

1 *See* LAWRENCE A. GORDON ET AL., COMPUTER SECURITY INSTITUTE, 2004 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 11 fig.16 (2004), *at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf [hereinafter 2004 CSI/FBI SURVEY].

2 On the problems of computer security in networked environments, see, for example, Ross Anderson, *Why Information Security is Hard – An Economic Perspective*, *at* www.acsac.org/2001/papers/110.pdf (last visited Jan. 23, 2005) (originally presented at the 17th Annual Computer Security Applications Conference, Dec. 10-14, 2001) (identifying various "incentive failures" in achieving secure network environments); Amitai Aviram & Avishalom Tor, *Information Sharing in Critical Infrastructure Industries: Understanding the Behavioral and Economic Impediments* (George Mason Law & Econ. Research Paper No. 03-30; Fla. St. U. College of Law Public Law Research Paper No. 103), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=427540 (last revised Feb. 23, 2004) (discussing reasons for suboptimal investments in network security); Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable* (U. Chicago Law & Econ., Olin Working Paper No. 217 (2d Ser.)), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=573502 (last revised Aug. 10, 2004) (focus-

Security Institute (CSI) and the Federal Bureau of Investigation (FBI) calls for a more sober assessment. Although the respondents reported fewer successful attacks on their computer systems than in previous years, over half of them admitted that they had experienced at least one incident of "unauthorized use" within the past year.[3] The variety of security incidents and the average losses associated with them provide some sense of the gravity of the situation: sabotage ($871,000); system penetration ($901,500); Web site defacement ($958,100); telecom fraud ($3,997,500); financial fraud ($7,670,500); theft of proprietary information ($11,460,000); denial of service attacks ($26,064,050); and, most seriously of all, viruses ($55,053,900).[4]

Even more striking than the frequency, variety, and severity of these incidents was the relatively low rate at which they were reported to law enforcement officials: In four out of five cases, the compromised organizations declined even to *report* such incidents to law enforcement.[5] This disclosure rate of 20% was the lowest since the CSI and FBI began compiling such information in 1999.[6] The rate at which compromised entities reported incidents of computer intrusions compares unfavorably to reporting rates for robbery (60.5%), burglary (54.1%), simple assault (42.1%), and even rape and sexual assault (38.5%).[7] Indeed, similarly low rates of reporting criminal offenses are to be found among the most vulnerable and marginalized members of American society: immigrants on temporary visas who have suffered from domestic violence (20.8%) and battered, undocumented immigrants (18.8%).[8]

What explains the profound reluctance of compromised corporations to report computer security incidents to law enforcement officials? In explaining their unwillingness to report, roughly half of the respondents in the

---

ing on the role of ISP immunity in contributing to network insecurity); and Douglas A. Barnes, Note, *Deworming the Internet*, 83 TEX. L. REV. 279 (2005) (addressing obstacles to producing software resistant to computer "worms").

3 2004 CSI/FBI SURVEY, *supra* note 1, at 8 fig.11. In 2003, the CERT Coordination Center, a federally funded research and development institute specializing in Internet security, received reports of over 130,000 incidents – a six-fold increase since 2000. *See* CERT/CC Statistics 1988-2004, http://www.cert.org/stats/cert_stats.html#incidents (last updated Oct. 19, 2004) (reporting 21,756 incidents in 2000 and 137,529 incidents in 2003). Several factors make it difficult to analyze these figures, including the possibility of shifts over time in the willingness of entities to report such events to the organizations conducting the surveys.

4 2004 CSI/FBI SURVEY, *supra* note 1, at 10 fig.15.

5 *Id.* at 13 fig.20.

6 Rates of reporting to law enforcement for the period 1999-2003 were as follows: 1999 (32%); 2000 (25%); 2001 (36%); 2002 (34%); and 2003 (30%). *Id.*

7 *See* SHANNAN M. CATALANO, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, CRIMINAL VICTIMIZATION, 2003, at 10 (2004), *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/cv03.pdf.

8 *See, e.g.*, Lesley E. Orloff et al., Recent Development, *Battered Immigrant Women's Willingness to Call for Help and Police Response*, 13 UCLA WOMEN'S L.J. 43, 68 (2003).

2004 CSI/FBI Survey cited as a "very important factor" their "perception" that "negative publicity would hurt their organization's stock and/or image."[9] Another 35% expressed concern that competitors would use information reported to law enforcement officials to their advantage. One in five stated that they had determined that civil – rather than criminal – remedies would best serve their interests. And another 18% of the organizations surveyed claimed to be unaware that law enforcement officials would even be interested in the intrusions that they had suffered.[10]

Amidst a continuing onslaught of "viruses," "worms," and other forms of "malware," computer security experts and legal scholars have begun to rethink the traditional bifurcated approach to network security, which has relied predominately on private investment in prevention and public investment in prosecution.[11] On the one hand, experts in computer security have questioned whether the billions of dollars spent by private companies on technologies designed to defend computer networks have been commensurate with the security that has actually been achieved.[12] On the other hand, legal commentators have identified a series of challenges associated with public prosecution of computer crimes, including not only the hesitancy of compromised entities to report security breaches, but also the forensic challenges of determining the originators and propagators of mali-

---

[9] Recent research supports the perception that public disclosure of computer security incidents negatively affects stock price. *See* Katherine Campbell et al., *The Economic Cost of Publicly Announced Security Breaches: Empirical Evidence from the Stock Market*, 11 J. COMPUTER SEC. 431 (2003) (cited in 2004 CSI/FBI SURVEY, *supra* note 1, at 16 n.4).

[10] 2004 CSI/FBI SURVEY, *supra* note 1, at 14 fig.21.

[11] "Viruses" and "worms" are self-replicating computer programs that can be designed to damage the computers that they "infect." *See* Wikipedia.org, *Computer Virus*, *at* http://en.wikipedia.org/wiki/Computer_virus (last visited Jan. 23, 2005) and *Computer Worm*, *at* http://en.wikipedia.org/wiki/Computer_worm (last visited Jan. 23, 2005). "Malware" refers "to any software designed to cause damage to a single computer, server, or computer network." Microsoft TechNet, *Defining Malware: FAQ*, *at* http://www.microsoft.com/technet/security/topics/virus/malware.mspx (last visited Jan. 23, 2005). Following Doug Lichtman and Eric Posner, I use the terms "virus," "worm," and "malware" to refer generally to "any category of malicious computer code that is propagated on the Internet, using or interfering with privately owned computer equipment, and done in a way such that the relevant private party has not given informed consent to that use or interference." Lichtman & Posner, *supra* note 2 (manuscript at 8).

[12] A 2003 study by PricewaterhouseCoopers concluded that, although businesses in North America spent roughly 50% more per capita on information security than companies elsewhere in the world, the investment "didn't make them any safer *per se*." Scott Berinato, *The State of Information Security 2003*, CSO MAG., Oct. 2003, *available at* http://www.csoonline.com/read/100103/survey.html. For discussions of the "cost-effectiveness" of network security, see, for example, Lawrence A. Gordon & Robert Richardson, *The New Economics of Information Security: Information-Security Managers Must Grasp the Economics of Security to Protect Their Companies*, INFORMATIONWEEK, Mar. 29, 2004, *at* http://www.informationweek.com/story/showArticle.jhtml?articleID=18402633 and Lawrence A. Gordon & Martin P. Loeb, *The Economics of Information Security Investment*, 5 ACM TRANS. ON INFO. & SYS. SEC. 438 (2002).

cious code, the difficulties of coordinating enforcement efforts across national boundaries, and the rudimentary nature of laws governing cybercrime in many foreign jurisdictions.[13]

In this climate of online risk, growing concern over the cost-effectiveness of defensive safeguards, and relative lack of interest in criminal prosecution, the recent release of a network security product that offers the capacity to launch "counterstrikes" against digital intruders has caused a considerable stir in the Internet security community. In March 2004, Symbiot, Inc. ("Symbiot"), based in Austin, Texas, announced its development of "the first IT security solution that can both repel hostile attacks . . . and accurately identify the malicious attackers in order to plan and execute appropriate countermeasures" – in the company's words, "effectively fighting fire with fire."[14] Although the precise technical details of Symbiot's various security "solutions" remain unclear, the company has stated that its technology could enable users to "reflect" electronic intrusions back on their originators, to "disable," "destroy," or "seize control" of the "attacking assets," or to launch "asymmetric counterstrikes" against the originators of network attacks and, conceivably, even against third parties that have unintentionally contributed to such attacks.[15]

It is not the intention of this paper to assess the technical capabilities, legality, or desirability of Symbiot's various proprietary technologies, whose precise methods of operation remain unknown and which are in a state of ongoing development.[16] Instead, the paper uses Symbiot's technology as a point of departure from which to assess, in a more general way, the legality and desirability of digital "counterstrikes" against hackers and

---

[13] *See, e.g.*, Orin S. Kerr, Essay, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005); Jason V. Chang, *Computer Hacking: Making the Case for a National Reporting Requirement* (Berkman Center for Internet & Society at Harvard Law School, Research Pub. No. 2004-07), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=530825 (last revised June 2, 2004); Curtis E.A. Karnow, Launch on Warning: Aggressive Defense of Computer Systems, http://islandia.law.yale.edu/isp/digital%20cops/papers/karnow_newcops.pdf (last visited Jan. 23, 2005) (unpublished paper presented at the CyberCrime and Digital Law Enforcement Conference sponsored by the Yale Law School Information Society Project, Mar. 26-28, 2004); and Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 HARV. J. L. & TECH. 699, 707-10 (1998), *available at* http://jolt.law.harvard.edu/articles/pdf/v11/11HarvJLTech699.pdf.

[14] *Symbiot Security Announces World's First Solution to Strike Back Against Network-Based Attackers; Aggressive New Rules of Engagement Established in "Information Warfare,"* BUS. WIRE, Mar. 4, 2004, *at* http://www.findarticles.com/p/articles/mi_m0EIN/is_2004_March_4/ai_113905129. *See also Symbiot Announces General Availability of iSIMS*, BUS. WIRE, Apr. 1, 2004, *at* http://www.findarticles.com/p/articles/mi_m0EIN/is_2004_April_1/ai_114800004.

[15] Symbiot, Inc., Graduated Response™, *at* http://symbiot.com/graduatedres.html#CYCLE (last visited Aug. 3, 2004) (on file with author).

[16] The company has products in various stages of development. *See, e.g.*, Symbiot, Inc., Symbiot 7200: Solutions / Symbiot 7200, *at* http://www.symbiot.com/7200riskmetricssolutions.html (last visited Jan. 23, 2005) and Symbiot 9600: Solutions / Symbiot 9600, *at* http://www.symbiot.com/9600riskmetricssolutions.html (last visited Jan. 23, 2005).

third-party intermediaries (or "zombies").[17] As we shall see, the paper rejects both the position that parties should be privileged to engage in digital counterstrikes and the position that digital counterstrikes should be completely prohibited. Instead, the article proposes a middle course: Although proportionate counterstrikes against persons who intentionally propagate malware should be privileged, similar counterstrikes against unwitting third-party "zombies" should be subject to a liability rule by which the counterattacking party would be required, in most instances, to pay damages to the third party.

Part I introduces Symbiot's technology and philosophy as set forth in the company's recent public pronouncements. Broadening its focus beyond Symbiot's proprietary technology, Part II examines the main practical and legal challenges facing digital "counterstrike" technologies. Part III then explores a historical analog to the problem of unauthorized access to computer networks: the debate in early nineteenth-century England about the use of "spring guns" to deter persons seeking unauthorized access to land and game. Finally, Part IV offers some preliminary assessments concerning what type of legal regime might best govern the phenomenon of digital "counterattacks."

I. THE PROSPECTS OF COUNTERSTRIKE TECHNOLOGIES

To be sure, digital self-help – even in its "offensive" guise – did not begin with Symbiot. To the contrary, Symbiot itself has claimed that "[o]ne dirty little secret of information security is that corporations have been using 'tiger teams' for years in order to launch highly aggressive counterstrikes against attackers" and that "[t]he counterstrike capabilities of the U.S. Defense Department are even more advanced than corporate practices."[18] Although parties seldom admit to engaging in such measures,

---

[17] Distributed denial of service (DDoS) attacks typically "involve unauthorized intruders commandeering the computers of unsuspecting users and using these distributed systems, referred to as 'zombies,' to flood a particular website or service provider with junk messages." Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 245 n.41 (2003).

[18] Paco Nathan, *What "Countermeasures" Really Means*, O'REILLY.COM, Aug. 3, 2004, *at* http://www.onlamp.com/pub/a/security/2004/08/03/symbiot.html. In the context of information technology, a "tiger team" traditionally refers to a group of experts hired to expose vulnerabilities in the security of one's own network, not necessarily that of an adversary. *See* Whatis.com, *Tiger Team*, *at* http://whatis.techtarget.com/definition/0,,sid9_gci213146,00.html (last visited Jan. 23, 2005). For a recent glimpse of military cyberwarfare strategy, *see* Norman R. Howes, Michael Mezzino & John Sarkesain, On Cyber Warfare Command and Control Systems, *at* www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/118.pdf (last visited Jan. 23, 2005) (unpublished paper presented at the 9th International Command and Control Research and Technology Symposium in Copenhagen, Denmark, Sept. 14-16, 2004).

fragmentary evidence suggests that such efforts are not unknown. In December 1999, for example, Conxion, the company providing the Web-hosting service for the World Trade Organization, responded to a denial-of-service attack launched by a group of "electro-hippies" by reflecting the attack onto the e-hippies' server.[19] At times, cruder techniques have proved no less effective: An unnamed "senior security manager" at "one of the country's largest financial institutions" has reported visiting "the physical location" where a series of hacker attacks had originated, breaking in, stealing the offending computers, and leaving a note reading "See how it feels?" for the suspected wrongdoers.[20]

Nonetheless, Symbiot has claimed to offer the first commercially available technology specifically designed to permit its users to "strike back" against network intruders.[21] As such, it provides a particularly useful case study through which to examine both the possibilities and problems of digital counterstrike technologies.

A. *Symbiot's Technology*

As of January 2005, Symbiot offered a range of product "solutions," including the Symbiot 5600, styled by the company as "the most advanced risk detection and mitigation solution available on the market today."[22] Beginning in the first quarter of 2005, customers of Symbiot who purchased the Symbiot 5600 system were also to receive access to Symbiot.NET, a "central repository of attacker profiles based on the cooperative surveillance and reconnaissance gathered by all [of Symbiot's] network participants" that is "used to accurately identify attackers, evaluate their methods and intent, and recommend the appropriate countermeasures."[23]

For our purposes, the most fascinating aspect of Symbiot's portfolio of technologies is what it has described as its "iSIMS" (or "Intelligent Security

---

[19] *See* Pia Landergren, *Hacker Vigilantes Strike Back*, CNN.COM, June 20, 2001, *at* http://www.cnn.com/2001/TECH/internet/06/20/hacker.vigilantes.idg/ (discussing efforts of Conxion, the Department of Defense, and other entities to strike back at hackers). In Fall 1998, the Pentagon reportedly responded to an attack on one of its Web sites by "flood[ing] the browsers used to launch the attack with graphics and messages, causing them to crash." Winn Schwartau, *Striking Back: Corporate Vigilantes Go On the Offensive to Hunt Down Hackers*, NETWORKWORLDFUSION, Jan. 11, 1999, *at* http://www.nwfusion.com/archive/1999/54697_01-11-1999.html.

[20] Schwartau, *supra* note 19, at ¶¶ 6-9. The unnamed source also admitted to having resorted, on one occasion, "to baseball bats" on the theory that "[t]hat's what these punks will understand." *Id.* at ¶ 9.

[21] *Symbiot Security Announces*, *supra* note 14.

[22] Symbiot, Inc., Introducing the Symbiot 5600 – Featuring the Power of Risk Metrics, *at* www.symbiot.com/pdf/5600.pdf (last visited Jan. 23, 2005).

[23] *Id.* *See also* Symbiot, Inc., Symbiot.NET: Solutions / Symbiot.NET, *at* http://www.symbiot.com/symbiotnetriskmetricssolutions.html (last visited Jan. 23, 2005).

Infrastructure Management System") platform. According to informational materials distributed by the company, the iSIMS platform "features an intuitive command and control console that aggregates, correlates, and visualizes security event data in real-time." Symbiot assists its users in characterizing the risk associated with particular computer security incidents by generating a three-digit "standardized measure of threat" similar to the "credit scores" provided by credit reporting companies. The vulnerability of a particular network asset during a particular time period is modeled as a function of the threat, the asset's vulnerability, and the value of the asset at risk.[24]

Most notably, Symbiot has described iSIMS as "the only product . . . to offer customers graduated responses to deploy against network based attackers."[25] In prior public statements, Symbiot has described the iSIMS platform as enabling its users to engage in a series of "graduated countermeasures" depending on "the intensity, duration, and realized effect of hostile acts" and the degree of authorization provided by Symbiot.[26] Although the nature and effectiveness of these countermeasures remain unknown, they have been described in general terms by Symbiot as operating in the following ways: *Blocking Traffic* ("providing a brute-force wall of defense"); *Rate-limiting* ("adjusting the bandwidth available to the attacker"); *Diverting Traffic* ("redirecting traffic to some other target network"); *Simulated Responses* ("providing 'decoy' responses to service requests" that appear "legitimate" but do not "stress . . . critical servers"); *Quarantine* ("accepting the attack, but redirecting it into a special 'containment area'" for analysis of its "characteristics"); *Reflection* ("sending the packet content used in the attack back at the attacker"); *Tagging* ("using a means for marking the attacker with information" for the purpose of identifying "subsequent incidents"); and *Upstream Remediation* ("attempting remediation through an attacker's upstream provider").[27]

In a related portion of its informational materials, under a distinctive heading entitled "For Authorized Deployments Only," Symbiot has also identified three "more aggressive countermeasures" whose availability may be "restricted:" *Invasive Techniques* ("obtaining access privileges on the attacker's system, and then pursuing a strategy of disabling, destroying, or seizing control over the attacking assets"); *Symmetric Counterstrike* ("sending exploits and other attacks which are specific to vulnerabilities on the

---

[24] For details, see Symbiot, Inc., iSIMS Overview, *at* http://internet-security.ws/isims.pdf#CYCLE (last visited Jan. 23, 2005) (in possession of author) [hereinafter iSIMS Overview]; Andy Oram, *Symbiot on the Rules of Engagement*, O'REILLY.COM, Mar. 10, 2004, *at* http://www.onlamp.com/lpt/a/4691 (interview with Symbiot's chief officers); and Paco Nathan & William Hurley, *Non-Equilibrium Risk Models in Enterprise Network Security* (Nov. 28, 2004), *at* www.symbiot.com/pdf/nerm.pdf.

[25] iSIMS Overview, *supra* note 24.

[26] Graduated Response™, *supra* note 15.

[27] *Id.*

attacker's system, in an amount proportional to their current attacks"); and *Asymmetric Counterstrike* ("preemptive measures in response to distributed attacks orchestrated by a known source," with "retaliation" potentially "far in excess of the attack that the aggressor has underway").[28]

Symbiot has explained that "asymmetric counterstrikes" – the last and, apparently, most aggressive type of response – "require executive findings based on multiple attributions and prior failed attempts at resolution through upstream providers and local jurisdictions." In such instances, Symbiot has stated that the company's "operations center" might authorize "escalated multilateral profiling and blacklisting of upstream providers," "distributed denial of service counterstrikes," "special operations experts applying invasive techniques," and "combined operations which apply financial derivatives, publicity disinformation, and other techniques of psychological operations."[29]

B. *Symbiot's Philosophy*

Although such vague descriptions do little to clarify Symbiot's actual methods and technological capacities, the company's officers have spoken at some length about their philosophy in ways that potentially bear on how the law should respond to the promise and problems of digital counterstrike technologies.

In an article published in August 2004, for example, Paco Nathan (Symbiot's Chief Scientist and Vice President of Research and Development) observed that "[w]hen computer security professionals speak about countermeasures, the implications are more subtle than the general public might imagine."[30] As if to allay concerns about the risks of iSIMS-enabled counterstrikes, Nathan provided the following assurances:

> Does it mean that if your grandmother's PC gets a virus, it could be accidentally "neutralized" and all her special cookie recipes obliterated? No. It *does* mean that if she neglects to clean up a bunch of viruses on her hard drive, she might encounter difficulties shopping online. Furthermore, if your grandmother chooses to go online through a cut-rate ISP with a history of sheltering attacks, she will probably have her bandwidth limited by web sites that take security seriously.[31]

Thus, Nathan draws a potentially important distinction between counterstrikes that result in permanent destruction of data and those that merely result in limiting the bandwidth of individuals who propagate – even

[28] *Id.* *See also* Lyne Bourque, *Symbiot iSIMS: The Counterattack*, EITPLANET.COM, June 29, 2004, *at* http://www.enterpriseitplanet.com/security/features/article.php/3374971.

[29] Paco Nathan & Mike Erwin, *On the Rules of Engagement for Information Warfare* 4-5 (Mar. 4, 2004), *at* http://www.symbiot.com/pdf/iwROE.pdf.

[30] Nathan, *supra* note 18, at ¶ 2.

[31] *Id.* at ¶ 13 (emphasis added).

result in limiting the bandwidth of individuals who propagate – even unintentionally – viruses, worms, and other forms of malware.

In other public statements, Symbiot has defended the moral and legal legitimacy of digital counterstrikes. The chief vehicle for this campaign is a document entitled "On the Rules of Engagement for Information Warfare," which Symbiot made available online in March 2004 shortly before the release of iSIMS.[32] Drawing upon doctrines of international law, Symbiot's "Rules of Engagement" contend that digital counterstrikes – at least as contemplated by Symbiot – are both principled and legal because they subscribe to "the lawful military doctrine of *necessity and proportionality*." According to Symbiot:

> Necessity is defined by the determination of hostile intent and the subsequent use of force in self-defense, justified in situations that are "instant, overwhelming and leaving no choice of means and no moment for deliberation." Proportionality is defined by the limitation of response by the intensity, duration, and realized effect of each attack.[33]

Purporting to rely on "strategies and tactics . . . refined by thousands of years of warfare, diplomacy, and legal recourse," Symbiot's "Rules of Engagement" seek to provide both moral and legal justification for the company's proprietary technology.[34]

II. THE PITFALLS OF COUNTERSTRIKE TECHNOLOGIES

How well have Symbiot's technical, moral, and legal claims been received? Most commentators who have reacted to Symbiot's iSIMS technology have expressed considerable concern about its possible use.[35] This

---

[32] Nathan & Erwin, *supra* note 29.

[33] *Id.* at 2-3 (internal citation removed). The quotation, as Symbiot notes, is from former U.S. Secretary of State Daniel Webster during the *Caroline* Affair. In 1837, the *Caroline*, an American ship being used to transport supplies from New York to a group of armed rebels preparing to invade Canada, was attacked, burned, and thrown over Niagara Falls by a Canadian naval force. British politicians defended the Canadians' actions as self-defense. Webster, by contrast, argued that the perpetrators had not demonstrated the "necessity" of self-defense because they had not responded to a threat that was "instant, overwhelming, leaving no choice of means, and no moment for deliberation." Enclosure (dated Apr. 24, 1841) in Letter from Daniel Webster to Lord Ashburton (July 27, 1842), *available at* http://www.yale.edu/lawweb/avalon/diplomacy/britian/br-1842d.htm#web2 (last visited Jan. 23, 2005).

[34] Nathan & Erwin, *supra* note 29, at 1.

[35] For responses to Symbiot's announcement of the release of iSIMS, see Munir Kotadia, *Security Product to Strike Back at Hackers*, CNET NEWS.COM, Mar. 10, 2004, *at* http://news.com.com/2102-7349_3-5172032.html; Dana Epps, *Rules of Engagement for Information Warfare*, SilverStr's Blog, Mar. 10, 2004, *at* http://silverstr.ufies.org/blog/archives/000547.html; Mike Fratto, *Fundamentals – Retaliation Is Not the Answer*, SEC. PIPELINE, Apr. 15, 2004, *at* http://www.securitypipeline.com/trends/showArticle.jhtml?articleId=18901411; Matthew Fordahl, *Vigilante Justice In Cyberspace*, CBSNEWS.COM, June 21, 2004, *at*

caution appears consistent with the position taken by most corporate executives, who have been reluctant – at least publicly – to support digital counterstrikes as a means of combating network-related intrusions.[36] The Department of Justice, for its part, has seemingly "taken a position unequivocally opposed to the employment of active defenses," both because of perceived challenges in "controlling" so-called "hack back" technologies and because such measures might themselves violate existing laws prohibiting unauthorized access to protected computers.[37]

Broadening our focus beyond Symbiot's proprietary technology, what are the chief practical and legal pitfalls facing companies that wish to launch digital counterstrikes?

A. *Practical Pitfalls*

Experts in computer security have focused principally on the practical risks associated with the use of so-called "hack back" technologies. Some have suggested that electronic countermeasures could slow networks by taking up valuable bandwidth.[38] Most frequently, however, technical experts have expressed concern that digital counterstrikes might harm "innocent" third parties, especially because persons engaged in unlawful online activities frequently route their attacks through passive intermediaries. Once infected, these so-called "zombie" computers can then be controlled by the originator of a worm or virus (the "zombiemaster") and be instructed to disseminate malicious code at some future time.

In recent years, computers in homes, research universities, and even the United States Senate and Department of Defense have been transformed

---

http://www.cbsnews.com/stories/2004/06/21/tech/main625144.shtml; and *System Attacks Back at Hackers,* BLACKCODE NEWS, June 20, 2004, *at* http://www.blackcode.com/news/view.php?id=487.

[36] *See (Too) Risky Business,* CSO MAG., Nov. 2003, *available at* http://www.csoonline.com/read/110103/digex_sidebar_1898.html and Deborah Radcliff, *Hack Back: Virtual Vigilante or Packet Pacifist? Network Executives Have Mixed Feelings About Whether to Retaliate Against an Attack,* NETWORKWORLDFUSION, May 29, 2000, *at* http://www.nwfusion.com/research/2000/0529feat2.html.

[37] Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?,* 22 HOUS. J. INT'L L. 223, 258 (2000). *Accord,* Emily Frye, Transcript of JLEP/CIPP Symposium on Property Rights on the Frontier: The Economics of Self-Help and Self-Defense in Cyberspace 212 (Sept. 10, 2004) (recounting discussions of counterstrike technology with officials in the Computer Crimes Division of the Department of Justice who, in Frye's words, "are not in favor of it") [hereinafter Symposium Transcript].

[38] *See* Sharon Gaudin, *Plan to Counterattack Hackers Draws More Fire,* INTERNETNEWS.COM, Apr. 5, 2004, *at* http://www.internetnews.com/ent-news/print.php/3335811 (addressing issues of "network traffic" and "corporate bandwidth").

into "zombies" in this manner.[39] A prominent legal practitioner has summarized the dangers as follows:

> [Z]ombies in a DDoS attack, may be operated by hospitals, governmental units, and telecommunications entities such as Internet service providers that provide connectivity to millions of people: counterstrikes which are not *very, very* precisely targeted to the worm or virus could easily create a remedy worse than the disease.[40]

In the worst case, as Orin Kerr has suggested, counterstrikes could resemble a "piñata game" in which the counterattacker "hacks" blindly at an unseen target.[41]

Symbiot, for its part, has publicly addressed such concerns. In an interview granted in March 2004, the company's chief officers noted that, "when there is no positive identification of the attacker (that is, we cannot positively attribute an attack back to its source), deploying defensive countermeasures and reporting intelligence would be most appropriate."[42] But the company has also acknowledged that "[t]here is always the possibility of collateral damage." Indeed, Symbiot makes no apologies for the possibility that counterstrikes might be launched against "zombies." According to Symbiot's officers, "when a zombied host or an infected computer has been clearly identified as the source of an attack, it is our responsibility to empower customers to defend themselves." Put simply, "[a]n infected machine, one no longer under the control of its owner, is no longer an innocent bystander."[43]

---

39 *See, e.g., Your Computer Could be a "Spam Zombie": New Loophole: Poorly Guarded Home Computers*, CNN.COM, Feb. 18, 2004, *at* http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/ (estimating "that between one-third and two-thirds of unwanted messages are relayed unwittingly by PC owners who set up software incorrectly or fail to secure their machines"); John Borland & John Pelline, *Hack Leads Point to California Universities*, CNET NEWS.COM, Feb. 12, 2000, *at* http://news.com.com/2100-1023-236827.html?legacy=cnet (referring to attacks against Yahoo!, eBay, CNN, and other companies unintentionally launched from computers at Stanford, UCLA, and the University of California at Santa Barbara); and Jon Swartz, *Hackers Hijack Federal Computers*, USATODAY.COM, Aug. 30, 2004, *at* http://www.usatoday.com/tech/news/computersecurity/2004-08-30-cyber-crime_x.htm (discussing recent discovery by officials at the Department of Justice of "[h]undreds of powerful computers at the Defense Department and U.S. Senate . . . hijacked by hackers who used them to send spam").

40 Karnow, *supra* note 13 (manuscript at 4-5) (emphasis added).

41 "It's . . . like, I think, a piñata game. You know the piñata game, where you blindfold somebody and give them a baseball bat and tell them to hack at the piñata." Orin S. Kerr, Symposium Transcript, *supra* note 37, at 231.

42 Oram, *supra* note 24.

43 *Id.*

B. *Legal Pitfalls*

Other critics of digital counterstrike technologies have argued that, even if such attacks could be conducted with technical precision, they are likely to run afoul of existing laws prohibiting unauthorized access to computers.

The most obvious – though by no means the only – challenge in this regard is the federal Computer Fraud and Abuse Act (CFAA), by which persons engaged in various forms of "unauthorized access" to computer systems face exposure to both civil and criminal liability.[44] The broad language of the CFAA prohibits both (1) "knowingly caus[ing] the transmission of a program, information, code, or command, and . . . intentionally caus[ing] damage . . . to a protected computer" and (2) "intentionally access[ing] a protected computer without authorization, and . . . recklessly caus[ing] damage."[45] Given the broad and evolving contours of the CFAA, some commentators have suggested that even the relatively benign attempt to *trace* an originator of a computer-related attack through various intermediaries might run afoul of the statute.[46]

For its part, Symbiot has conceded that "[t]he legal environment surrounding the use, misuse, and operation of a system for active network self-defense has many unexplored issues."[47] Although it is impossible to evaluate such issues thoroughly without more information about a given technology's mode of operation once actually deployed, the types of counterstrikes identified by Symbiot (which include "disabling, destroying, or seizing control" over "attacking assets") could conceivably run afoul of provisions in the CFAA.

To date, no court has considered whether digital counterstrikes of the type described by Symbiot violate the CFAA or, for that matter, any other federal or state law. Accordingly, to better assess the legality and desirability of digital counterstrikes in this unsettled area of the law, we turn to a historical analog: the controversy over the use of "spring guns" to combat illegal poaching in nineteenth-century England.

---

[44] 18 U.S.C. § 1030 (2002). Possible exposure to an action under the CFAA by no means exhausts the sources of potential liability. For an overview, see Karnow, *supra* note 13 (manuscript at 5) (noting that "a host of statutes on their face make it illegal to attack or disable computers").

[45] 18 U.S.C. § 1030(a)(5)(A)(i)-(ii).

[46] "Insofar as private security experts may lack authorization to enter third-party systems, even for investigative purposes, some of the law's prohibitions may impact attempts by private parties to trace and identify unauthorized intruders." Mitchell & Banker, *supra* note 13, at 711. For discussions of the CFAA's scope, see generally Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) and Robert Ditzion, Elizabeth Geddes & Mary Rhodes, *Computer Crimes*, 40 AM. CRIM. L. REV. 285 (2003).

[47] Although Symbiot's officers have taken the position that "legal liability is borne by the attacker" [i.e., their customer], they have acknowledged that "[t]he legal implications . . . and liabilities arising from the system's use are presently very important for us all to consider." Oram, *supra* note 24.

III. POACHERS AND SPRING GUNS

Like modern-day network security specialists, the owners of English landed estates in the eighteenth and early-nineteenth centuries resorted to a range of defensive self-help measures designed to protect their property and game from unauthorized intruders. Like today, English landowners sought to protect certain things of value (such as deer and birds) whose status as "property" was contested. Like their modern-day counterparts, owners of land periodically resorted to civil and criminal actions against intruders.[48] Moreover, as with proponents of digital counterstrike technologies, property owners in England engaged in various forms of self-help – most notoriously, the placement of spring guns and other mechanical devices designed to retaliate against unauthorized intruders. And, as in the modern age, such devices generated considerable controversy because of the risks that they posed to innocent third parties. With the modern problem of digital self-help in mind, Part III examines the nineteenth-century English spring gun controversy and its later analysis by twentieth-century scholars of law and economics.

A. *The History of Spring Guns*

As Judge Posner has observed, the use of self-help measures to deter poachers became a "*cause célèbre*" in England in the 1820s, occupying the English judiciary, legislature, and press.[49] The debates focused on the use of three types of devices: "spring guns" (designed to discharge automatically when "sprung" by the entry of an intruder); "man traps" (intended to snap on the legs of intruders – or their dogs); and "dog spears" (fashioned to impale dogs employed in the hunting of game upon sharpened metal stakes).

The highlights of the controversy have been explored elsewhere and need only be broached briefly here.[50] In *Ilott v. Wilkes* (1820), the Court of

---

[48] Civil actions in such cases might be brought for trespass. Criminal prosecutions might occur in summary (i.e., non-jury) proceedings before justices of the peace or before juries under the notorious Black Act, which defined various types of poaching-related acts as felonies punishable by death. *See generally* PETER B. MUNSCHE, GENTLEMEN AND POACHERS: THE ENGLISH GAME LAWS, 1671-1831 (1981) and E.P. THOMPSON, WHIGS AND HUNTERS: THE ORIGIN OF THE BLACK ACT (1975).

[49] Richard A. Posner, *Killing or Wounding to Protect a Property Interest*, 14 J.L. & ECON. 201, 202 (1971).

[50] This is not to say, however, that they have always been chronicled accurately. For example, a leading casebook on American tort law has placed the important case of *Bird v. Holbrook* (decided in 1828) in 1825 and the most important Parliamentary act regulating "spring guns" and "man traps" (adopted in 1827) in 1826. *See* RICHARD A. EPSTEIN ET AL., CASES AND MATERIALS ON TORTS 40-43 (7th ed. 2000). The book also claims that the statute concerning spring guns and man traps adopted in 1827 was "repealed in its entirety in 1861" – which indeed it was – but it fails to note that the main

King's Bench took up the question of whether a trespasser who had been *warned* that spring guns had been placed in a wooded tract could maintain an action against the property owner for injuries sustained by entering the property and activating a gun, one of "nine or ten" that had been placed on the property by the owner.[51] In deciding whether a cause of action by the trespasser could lie, Chief Justice Abbott observed that the judges were "not called upon . . . to decide the *general* question, whether a trespasser sustaining an injury from a latent engine of mischief, placed in a wood or in grounds *where he had no reason to apprehend personal danger*, may or may not maintain an action."[52] But in the case where actual notice did exist, the Court of King's Bench determined that no action for injuries caused by the gun could be maintained.[53]

After the decision in *Ilott*, debate concerning the regulation of spring guns shifted to Parliament. Opponents of spring guns argued that the devices had the tendency to harm innocent victims – including children, persons who entered property "by accident," those who ventured in "with some kind and friendly purpose," and even gamekeepers themselves.[54] Proponents of spring guns claimed that the devices "not only acted as a great discouragement to poaching, but tended to prevent the dreadful evils which resulted from the affrays and fights between bodies of game-keepers and

---

provisions of the 1827 statute were included in a separate consolidated act passed in that same year. *Id.* at 44 n.1. For the consolidating measure, see Offenses Against the Person Act, 1861, 24 & 25 Vict., c. 100, § 31 (Eng.). These infelicities do little to detract from Professor Epstein's influential casebook, which remains a "classic."

[51] 106 Eng. Rep. 674 (K.B. 1820). The defendant in *Ilott* owned a wooded tract of land that contained "a right of way for all the king's subjects on foot." *Id.* at 675. He placed guns on the private portions of the land and displayed several "boards" that contained "notice to the public that such instruments were so placed." *Id.* The plaintiff and a companion "went out in the day time for the purpose of gathering nuts," and the plaintiff "proposed to his companion to enter" the defendant's woods. *Id.* After being warned by his companion, the plaintiff entered, whereupon he received the injury at issue in the suit. *Id.*

[52] *Id.* at 676 (emphasis added). That particular question, as the Chief Justice observed, "ha[d] been the subject of much discussion in the Court of Common Pleas, and great difference of opinion ha[d] prevailed in the minds of the learned judges, whose attention was there called to it." *Id.* *See* Deane v. Clayton, 129 Eng. Rep. 196, 197 (C.P. 1817) (failing to reach decision on the issue of whether an action could be brought by a plaintiff whose dog had been killed by dog spears).

[53] *Ilott*, 106 Eng. Rep. at 676. Justice Bayley, for his part, agreed, noting that the action was barred by the maxim of *volenti non fit injuria* and concluding that "the cause of the injury" was ultimately the act of the plaintiff, not the defendant. *Id.* at 677-78 (Bayley, J.)

[54] 13 PARL. DEB. (2d. ser.) (1826) 1254-55 (Charles Tennyson). In 1818, the *Bury and Norwich Post* reported a typical accident involving an injured gamekeeper:

On Saturday . . . George Davex, gamekeeper to Miss Wenyeve of Brettenham Hall was in the act of taking up a spring gun set by himself, from touching a wire too roughly, he sprang the lock and the contents of the gun lodged in various parts of his body from head to foot.

Bury and Norwich Post (Mar. 25, 1818), *available at* http://www.foxearth.org.uk/1818-1819BuryNorwichPost.html.

poachers" – in effect, *reducing* interpersonal violence.[55] In May 1827, after several years of intermittent debate, Parliament ultimately enacted a statute that made it a misdemeanor for any person to "set or place or cause to be set or placed, any Spring Gun, Man Trap, or other Engine calculated to destroy human Life, or inflict grievous bodily Harm, . . . upon a Trespasser or other Person coming in contact therewith."[56]

English judges promptly took notice.[57] In *Bird v. Holbrook* (1828), the Court of Common Pleas considered the case of a plaintiff who had been injured by a spring gun after climbing into the defendant's walled garden to retrieve a pea-fowl that had strayed.[58] The owner of the garden, who had recently experienced the theft of flowers, had not only placed a spring gun, but had intentionally declined to post any notice to that effect. After entering the garden to retrieve his bird, the plaintiff was shot in "the knee-joint" and suffered "a severe wound."[59] Noting that the recently adopted Parliamentary act of 1827 prohibited the setting of spring guns "even with *notice*, except in dwelling-houses by night," Chief Justice Best concluded that the action could be maintained by the plaintiff.[60] As the court observed, "he who sets spring guns, without giving notice, is guilty of an inhuman act, and that, if injurious consequences ensue, he is liable to yield redress to the sufferer."[61]

B. *The Law and Economics of Spring Guns*

Although of relatively modest interest to legal historians, the English spring gun debate has been familiar to scholars of law and economics since 1971, when it was first explored by Judge Posner in an incisive article pub-

---

55 13 PARL. DEB. (2d ser.) (1826) 1266-67 (Stuart Wortley).

56 7 & 8 Geo. IV, c. 18, § 1 (1827) (Eng.). The act also covered those who "knowingly and wil[l]fully" permitted such devices to remain in place after they had been set by others. *Id.* § 3. Notably, the act excluded spring guns, man traps, or other "engines" set "from Sunset to Sunrise" in dwelling houses. *Id.* § 4.

57 The impact on Anglo-American landowners, however, is more difficult to assess. The American case law certainly suggests that innovative self-help strategies persisted. *See, e.g.*, Johnson v. Patterson, 14 Conn. 1 (1840) (corn laced with arsenic placed by defendant on his land); Grant v. Hass, 75 S.W. 342 (Tex. Civ. App. 1903) (spring gun designed to deter the theft of melons); and Katko v. Briney, 183 N.W. 2d 657 (Iowa 1971) (spring gun designed to protect an unoccupied boarded-up farm house against trespassers and thieves). My maternal grandfather George Smillie employed a spring gun loaded with powder in the shed that adjoined his cottage in southern Quebec to prevent depredations when the premises were unoccupied during winter.

58 Bird v. Holbrook, 130 Eng. Rep. 911, 913 (C.P. 1828).

59 *Id.*

60 *Id.* at 916 (emphasis added).

61 Id.

lished in the *Journal of Law and Economics*.[62] Reflecting the influence of Coase, Posner styled the dispute in *Bird v. Holbrook* as a simple "conflict between [two] legitimate activities" – tulip growing and peahen keeping. In turn, he characterized the use of spring guns as a rational reaction to the rudimentary policing of nineteenth-century rural England: "In an era of negligible police protection, a spring gun may have been the most cost-effective means of protection for the tulips."[63]

Posner ultimately fashioned the following six-part test to determine whether violence in defense of property should be permitted:

(1) Deadly force should not be privileged where the property owner has an adequate legal remedy or where "the threatened property loss is small;"

(2) There should be no privilege to set spring guns "in heavily built-up residential and business areas" because of the likely presence of police and the increased risk of third-party injury;

(3) The privilege to use deadly force to defend property should be forfeited "if the user fails to take reasonable precautions to minimize the danger of accidental injury;"

(4) With respect to property "not sufficiently enclosed to keep out straying animals, children, and youths, the privilege to set spring guns should be limited to the nighttime;"

(5) In situations where deadly force is permissible, "[a]n adult intruder killed or injured in an attempt to steal or destroy property should not be permitted to recover damages" and "[a]n innocent intruder should be denied recovery if carelessness on his part contributed materially to the accident;" and

(6) In cases where neither the landowner nor the innocent intruder had been "demonstrably careless," losses should be borne by the *property owner* because he or she was likely to be in a better position to assess and monitor the hazards.[64]

Under the multi-part test articulated by Posner, "neither blanket permission nor blanket prohibition of spring guns and other methods of using

---

62 *See* Posner, *Killing or Wounding*, *supra* note 49. *See also* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 225 (5th ed. 1998) and EPSTEIN ET AL., *supra* note 50, at 43-44.

63 POSNER, ECONOMIC ANALYSIS, *supra* note 62, at 225. For a particularly scathing indictment of Posner's analysis of the *Bird* case, see Peter Read Teachout, *Worlds Beyond Theory: Toward the Expression of an Integrative Ethic for Self and Culture*, 83 MICH. L. REV. 849, 882 (1985) (reviewing JAMES BOYD WHITE, WHEN WORDS LOSE THEIR MEANING: CONSTITUTIONS AND RECONSTITUTIONS OF LANGUAGE, CHARACTER, AND COMMUNITY (1984)) ("What is most striking about the vision of the world expressed here is that it leaves out entirely the central fact of individual human suffering. What the case 'involved,' Posner insists without apparent embarrassment, is simply the question of which of two economic activities, tulip raising or peahen keeping, would be advantaged by drawing the liability rules one way or another. In his utter preoccupation with the efficiency question . . . he virtually steps over the body of the seriously maimed young man.").

64 Posner, *Killing or Wounding*, *supra* note 49, at 214-16.

deadly force to protect property interests is likely to be the rule of liability that minimizes the relevant costs."[65] Decision-makers, in short, must muddle through as best they can.

IV. TOWARDS A LEGAL REGIME FOR DIGITAL COUNTERSTRIKES

But how should policy makers muddle through the issue of digital countermeasures? And does the law-and-economics analysis of spring guns provide any guidance as to the appropriate contours of digital self-help?

Part A examines the extent to which the things that English landowners sought to protect from unauthorized access (i.e., land and game) can be considered analogous to the things that modern-day computer security specialists seek to protect (i.e., computer systems). Part B takes up the question of whether organizations whose computer systems have been attacked should be permitted to strike back against hackers and third-party "zombies."

A. *Land, Game, and Computer Systems*

Before proceeding further, we would be well served to ask a pair of vexing questions: Can computer systems be analogized profitably to real property or animals? And, if so, do the rights associated with property ownership have any relevance to the problem of unauthorized intrusion to computer systems?

As Richard Epstein has observed, the "equipment and facilities" that comprise the Internet "are not by any stretch of the imagination real property."[66] Nonetheless, as Epstein has argued, networked computers can profitably be viewed as "a new form of chattel."[67] And much like eighteenth-century English Parliamentarians expanded the law of theft to protect certain things of value (such as metal fixtures, crops, or animals) traditionally outside the law of larceny,[68] twenty-first century jurists have "breathed new life into the common law" by rendering an ancient doctrine – trespass to chattels – "viable" in the digital world.[69]

As applied to various types of unauthorized access, the operator of a computer system that alleges a claim of trespass to chattels generally must establish that the defendant intentionally "intermeddled" with the plaintiff's

---

65 *Id.* at 214.

66 Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 76 (2003).

67 *Id.*

68 On these Parliamentary efforts, see Bruce P. Smith, *The Presumption of Guilt and the English Law of Theft, 1750-1850*, 23 LAW & HIST. REV. 133 (2005).

69 Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 436 (2d Cir. 2004).

chattel – in this case, their computer system.[70] The recent case of *Register.com, Inc. v. Verio, Inc.* (2004), decided by the U.S. Court of Appeals for the Second Circuit, is illustrative.[71] In *Register.com*, the defendant was accused of accessing the plaintiff's database of domain names by means of robotic searches. In considering Register.com's theory of trespass to chattels, the appellate court first determined that the plaintiff's computer systems qualified as chattels. The appellate panel then concluded that Verio had likely committed a trespass to chattels by using its robot "to access Register.com's computer systems without authorization to do so, consuming the computer systems' capacity." In concluding that the district court had not abused its discretion in granting preliminary relief on the plaintiff's trespass to chattels claim, the appellate court observed that Register.com's computer systems were "valuable resources of finite capacity," that "unauthorized use of such systems deplete[d] the capacity available to authorized end-users," that unauthorized use "create[d] risks of congestion and overload that may [have] disrupt[ed] Register.com's operations," and that the district court had concluded that the plaintiff would suffer irreparable harm.[72]

On the whole, decisions that have imported property-related concepts into cases involving unauthorized online intrusions have not sat well with scholars of Internet law, who have contended that the "propertization" of the Internet will stifle expression, create a digital "anti-commons," and curtail the public domain.[73] With that said, other scholars have recognized the appeal of property-related metaphors to judges and even the desirability of extending them further.[74] Even Dan Burk, who, in influential article, has

---

70 RESTATEMENT (SECOND) OF TORTS § 217 (1965). For representative cases, see, for example, *Register.com*, 356 F.3d 393 (affirming preliminary injunction on trespass to chattels theory based on defendant's use of search robots to access plaintiff's database); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (affirming preliminary injunction based on allegation of trespass to chattels in case involving robotic copying of auction-related information); Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724, 2001 U.S. Dist. LEXIS 22520 (N.D. Cal. 2001) (refusing to dismiss claim in case involving copying of metatag information by software robot); AOL, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998) (finding liability on trespass to chattels theory in case of spam); and Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996) (applying trespass to chattels theory in case involving unauthorized "cracking" of telephone access codes).

71 356 F.3d 393.

72 *Id.* at 438.

73 *See, e.g.*, Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53 (2000); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521 (2003); James Boyle, *The Public Domain: The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33 (2003); and Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 468 (2003).

74 *See, e.g.*, David McGowan, *The Trespass Trouble and the Metaphor Muddle*, 1 J.L. ECON. & POL'Y 109 (2005) (suggesting that property metaphors are more apt for the Internet than critics have suggested) and Adam Mossoff, *Spam – Oy, What a Nuisance!*, 19 BERK. TECH. L.J. 625, 664 (2004)

criticized application of the trespass to chattels doctrine to "exotic" and "dubious" computer-related cases, has acknowledged that "[o]ne could easily envision the application of this tort claim to a variety of computer-related situations in which unauthorized users *impaired* the function of a computer system, perhaps by damaging hardware or software, or even by locking the owner out of important computer files."[75]

Indeed, if one accepts that computer systems are a form of property, the malicious propagation of worms and viruses would appear to satisfy the two key elements of a trespass to chattels claim: first, the acts are likely to harm "the possessor's materially valuable interest in the physical condition, quality, or value of the chattel," to deprive the possessor of "the use of the chattel for a substantial time," or to affect "some other legally protected interest of the possessor;" and, second, persons who disseminate malware with the intent of "crashing" a computer system *intend* to intermeddle.[76] Thus, unlike cases where harm is "indirect"[77] or virtually impossible to discern,[78] cases in which entities have had their computer systems damaged or disabled by malware are likely to be in a strong position to prove intentional, direct, and significant harm.[79]

We linger on the tort of trespass to chattels not to suggest that it is a solution to the problem of unauthorized access or, for that matter, a substitute for self-help. To the contrary, companies who decline to report computer security incidents to law enforcement authorities may find the prospects of a trespass-related *civil* suit no more palatable. Yet while conceptualizing unauthorized access to computer systems as a tortious harm to "property" might appear to matter little to those companies disinterested in civil litigation, thinking about such harms as *property*-related harms may provide such companies with latitude to engage in meaningful forms of self-help.

Consider Section 218 of the *Restatement (Second) of Torts*, which describes the prerequisites for a finding of liability on a claim of trespass to

---

(arguing for extension of nuisance law to problem of spam on the grounds that the common law can both "protect legal entitlements, such as the right to use and enjoy one's property without substantial interference, and . . . redress new forms of injury, such as the harmful effects of spam.").

75 Burk, *supra* note 73, at 28-29 (emphasis added).

76 RESTATEMENT (SECOND) OF TORTS § 218 (1965).

77 *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296, 308 (Cal. 2003) ("Intel's theory would expand the tort of trespass to chattels to cover virtually any unconsented-to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter.").

78 *See, e.g.*, Ticketmaster, Corp. v. Tickets.com, Inc., 2003 U.S. Dist. LEXIS 6483, No. CV99-7654-HLH(VBKx) (C.D. Cal. Mar. 7, 2003), at *12 ("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.").

79 *See, e.g.*, Physicians Interactive v. Lathian Sys., 2003 U.S. Dist. LEXIS 22868, No. CA-03-1193-A (E.D. Va. Dec. 5. 2003), at *26 (finding that alleged "attacks" by defendants on file servers "were designed to intermeddle with personal property").

chattels. Viewed from one perspective, Section 218 seems to constrict the options of property owners, since it suggests that a party seeking to establish the defendant's "intermeddling" for purposes of a civil suit must establish more than trivial damage. Yet, as David McGowan has observed, comment e to Section 218 also makes clear that the possessors of chattels retain the "privilege to use reasonable force" to protect their possessions – even against those "harmless" interferences for which a formal legal action would be unavailing.[80] In declaring that property owners are privileged to use "reasonable force" to protect their possessions, comment e also refers its readers to Section 77 of the *Restatement*. Section 77 likewise permits property owners to engage in forceful self-help – provided the intrusion is not "privileged," the property owner "reasonably believes that the intrusion can be prevented or terminated only by the force used," and the property owner "has first requested the other to desist and the other has disregarded the request, or the actor reasonably believes that a request will be useless or that substantial harm will be done before it can be made."[81] And, finally, Section 84 authorizes the use of "mechanical devices not threatening death or serious bodily harm" to protect land or chattels "from intrusion" if the use of the device is "reasonably necessary to protect the . . . chattels from intrusion," the use is "reasonable under the circumstances," and "the device is one customarily used for such a purpose, or reasonable care is taken to make its use known to probable intruders."[82]

Considered together, these provisions would appear to provide considerable latitude to property owners to protect their property through various forms of self-help. But do they provide any guidance concerning the permissible scope of electronic counterstrikes designed to protect computer systems from intrusion?

B. *Counterstrikes Against "Hackers" and "Zombies"*

In working through the relevant issues, we might first envision the possibility of four basic types of legal regimes: (1) a regime that subjects counterstrikers to both criminal and civil liability; (2) one that privileges counterstrikers from criminal and civil liability; (3) one that imposes upon them criminal (but not civil) liability; or (4) one that imposes civil (but not criminal) liability. We might next consider two simplified situations: first, where a party has counterattacked against a "hacker" (a party that has inten-

---

80 RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965). *See also* McGowan, *supra* note 74.

81 RESTATEMENT (SECOND) OF TORTS § 77 (1965).

82 *Id.* § 84.

tionally engaged in illegal access); and, second, where a party has counterattacked against a "zombie" (an unwitting third-party intermediary).[83]

A reasonably strong case can be made that counterstrikes against "hackers" – at least when such measures are proportionate to the threat posed – should be privileged. As we have seen, Section 77 of the *Restatement (Second) of Torts* authorizes persons to use "reasonable force" to protect their property in instances where the intrusion is not "privileged," the property owner "reasonably believes that the intrusion can be prevented or terminated only by the force used," and the property owner "reasonably believes that a request will be useless or that substantial harm will be done before it can be made."[84] And Section 84 permits the use of "devices" to accomplish these ends – merely adding the requirement that "the device [be] one customarily used for such a purpose, or reasonable care [be] taken to make its use known to probable intruders."[85] Although it might well be the case that a party that "hacked back" against a network intruder might fall within the language of the CFAA or other statutes, the party would seem to possess a colorable claim – at least under traditional tort principles – that a proportionate counterstrike against a hacker should not expose the counterattacker to either criminal or civil liability.

But how should the law respond to the more difficult problem of counterstrikes against third-party "zombies," who have not engaged in intentional wrongs? As a normative matter, does it make sense for parties that counterstrike against "zombies" to be subjected to criminal and civil liability? With respect to potential criminal liability, a party engaged in digital counterstrikes might seek to invoke the "choice of evils" defense, which excuses certain apparently criminal acts if they are justified by the avoidance of greater harm – though the doctrine's application outside the realm

---

83 Although my usage of the term "hacker" to refer to persons engaged in unauthorized access by no means exhausts the term's varied meanings in the Internet context, it conforms with the conventions of the popular press. *See* Wikipedia.org, *Hacker*, *available at* http://en.wikipedia.org/wiki/Hacker (last visited Jan. 23, 2005).

84 *See supra* note 81 and accompanying text. Similarly, Section 3.06(1) of the Model Penal Code ("Use of Force Justifiable for Protection of Property") states that:

> [T]he use of force upon or toward the person of another is justifiable when the actor believes that such force is immediately necessary: (a) to prevent or terminate an unlawful entry or other trespass upon land or a trespass against or the unlawful carrying away of tangible, movable property, provided that such land or movable property is, or is believed by the actor to be, in his possession or in the possession of another person for whose protection he acts . . .

MODEL PENAL CODE § 3.06(1) (1985).

85 *See supra* note 82 and accompanying text. In turn, Section 3.06(5) of the Model Penal Code ("Use of Device to Protect Property") states that the section's justification extends to devices only if:

> (a) the device is not designed to cause or known to create a substantial risk of causing death or serious bodily injury; and (b) the use of the particular device to protect the property from entry or trespass is reasonable under the circumstances, as the actor believes them to be; and (c) the device is one customarily used for such a purpose or reasonable care is taken to make known to probable intruders the fact that it is used.

MODEL PENAL CODE § 3.06(5) (1985).

of immediate violence to *persons* remains unclear.[86] With respect to possible civil liability, a counterstriker could seek refuge under the doctrine of necessity – a principle, in the words of Professor Epstein, "as old as the doctrine of exclusive ownership itself."[87] As articulated in Section 197 of the *Restatement (Second) of Torts*, the doctrine of necessity states that "[o]ne is privileged to enter or remain on land in the possession of another if it is or reasonably appears to be necessary to prevent serious harm to . . . the actor, or his land or chattels. . . ."[88] Just as a sailor in peril is permitted to dock at another's wharf during a storm – even if damage to the dock might result – the operator of a computer system under siege might be permitted to "trespass" on the system of a third-party "zombie" even if it "damaged" the "zombie" by limiting or slowing its connection to the network.[89]

When confronted by cases in the "real" world, law-and-economics scholars have generally praised the decision of courts to permit parties to invoke the necessity doctrine in cases of intentional trespass – at least where the value to the trespasser is great, the costs of the trespass are modest, and the transactions costs associated with negotiations with the property owner whose property has been entered are high.[90] In the case of a party experiencing a DDoS attack, at least two of these elements would appear to be present: the cost of the incident to the party attacked is great; and the transaction costs of dealing with third-party "zombies" (given the typical case of a rapidly-propagating worm or virus) are likely to be high. Under this formulation of the rule, as long as the costs associated with the intrusion to the systems of third parties were "modest," counterstrikes against third parties would be permitted.

This does not mean, of course, that the costs of such trespasses should be borne by "zombies." As held in *Vincent v. Lake Erie Transportation Co.* (1910), a party that avails itself of the property of another and causes harm

---

[86] Section 3.02 of the Model Penal Code ("Justification Generally: Choice of Evils") states as follows:

> Conduct that the actor believes to be necessary to avoid a harm or evil to himself or to another is justifiable, provided that: (a) the harm or evil sought to be avoided by such conduct is greater than that sought to be prevented by the law defining the offense charged; and (b) neither the Code nor other law defining the offense provides exceptions or defenses dealing with the specific situation involved; and (c) a legislative purpose to exclude the justification claimed does not otherwise plainly appear.

MODEL PENAL CODE § 3.02 (1985).

[87] Richard A. Epstein, *Property and Necessity*, 13 HARV. J. L. PUB. POL'Y 2, 13 (1990) (demonstrating extent to which absolute property rights are qualified by necessity defense).

[88] RESTATEMENT (SECOND) OF TORTS § 197 (1965).

[89] *See* Ploof v. Putnam, 71 A. 188 (Vt. 1908) (remanding to trial court for determination of whether plaintiff could establish necessity of docking during storm).

[90] As Robert Cooter and Thomas Ulen have summarized, "the private-necessity doctrine allows compensated trespass in an emergency" on the grounds that "transaction costs may preclude bargaining." ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 161 (4th ed. 2002).

should be required to pay the costs of the damage.[91] The rule, in short, requires parties to internalize the costs of their actions. If digital counterstrikers accurately calculate the likely damage to themselves and third parties and rationally compare the estimates – assumptions that, admittedly, may be rather heroic given the uncertainties and time pressures involved in online attacks – the damages caused by digital countermeasures taken against third-party "zombies" will presumably be less than the costs borne by the party if it failed to counterstrike.[92]

How might the legal regime that has been outlined above affect the actual behavior of companies operating computer systems, persons interested in spreading malware, and third-party "zombies"? Predicting behavior in this area is perilous, but the following hypotheses seem plausible. The many companies that are currently reluctant to invoke formal law might be encouraged to take more active measures against hackers.[93] Although a hacker who encountered a computer system protected by a digital counterstrike technology might be diverted to a "softer" target or, alternatively, might be spurred to even more malicious ends, these consequences arguably would not arise if the technology were undetectable to the potential wrongdoer.[94] Indeed, like the LoJack car security system, which uses a series of hidden radio transceivers to permit law enforcement authorities to track and recover stolen automobiles, counterattacks that occurred without prior announcement to the hacker might actually reduce (and not simply displace) criminal wrongdoing.[95]

How, in turn, might potential "zombies" act in a legal regime that permitted, for example, counterattackers to limit their bandwidth or otherwise temporarily impair their "zombied" computer systems? As it currently stands, our legal regime provides virtually no incentives for vulnerable "zombies" to take even the most modest and inexpensive measures to pre-

---

91 124 N.W.2d 221 (Minn. 1910) (awarding damages to defendant whose dock was damaged by plaintiff's boat during storm). In the words of Judge Posner, "[s]uch liability is appropriate to assure that the rescue is really cost-justified, to encourage dock owners to cooperate with boats in distress, to get the right amount of investment in docks, . . . and, in short, to simulate the market transaction that would have occurred had transaction costs not been prohibitive." POSNER, ECONOMIC ANALYSIS, *supra* note 62, at 90-91.

92 This also assumes that parties engaging in counterstrikes can be identified and can pay for the damage they cause.

93 "[T]argets prefer self-help solutions in order to maintain a greater degree of confidentiality . . . than law enforcement typically allows." Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 197 (2000).

94 For a useful overview of the phenomenon of diversion, see Koo Hui-Wen & I.P.L. Png, *Private Security: Deterrent or Diversion?*, 14 INT'L REV. L. & ECON. 87 (1994).

95 *See* Ian Ayres & Steven D. Levitt, *Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack*, 113 Q. J. ECON. 43 (Feb. 1998). Ayres and Levitt found that car owners who install LoJack devices confer positive externalities by making auto theft "riskier and less profitable" and thus reducing auto theft in the aggregate. I am grateful to Richard McAdams for discussing this literature with me.

vent their systems from being compromised.[96] Upon initial examination, we might expect a regime that permitted third-party "zombies" to recover damages caused by counterstrikes to be little better. But just as compensation for dock owners provides them with an incentive to help boats in distress, damages payments to third-party "zombies" might encourage them to cooperate actively in responding to network-based attacks.[97] And just as third parties injured by spring guns might be barred from recovering damages if they had been "demonstrably careless," recovery by "zombies" could be barred or reduced in instances where such companies had failed to take reasonable security measures themselves.[98]

CONCLUSION

As this paper has suggested, self-help is alive and well in the Internet age.[99] In this regard, the area of computer security resembles other areas of American law – ranging from repossession, to bail enforcement, to self-defense against threats of immediate bodily harm – where self-help measures remain important.[100] Indeed, our current legal climate in the area of computer security bears certain resemblances to other contexts in which self-help has historically proved appealing, including "frontier" settings where formal legal systems were underdeveloped or non-existent,[101] instances where formal law proved incapable of providing adequate or af-

---

96 As a leading English network security expert has noted, although "computer users might be happy to spend $100 on anti-virus software to protect *themselves* against attack, they are unlikely to spend even $1 on software to prevent their machines being used to attack Amazon or Microsoft." Anderson, *supra* note 2 (manuscript at 1).

97 See supra note 91.

98 *See supra* note 64 and accompanying text.

99 *See also* Microsoft Corp., *Q&A: Microsoft Establishes Anti-Virus Reward Program*, Nov. 3, 2003, http://www.microsoft.com/presspass/features/2003/nov03/11-05AntiVirusQA.asp and Robert Lemos, *Mozilla Puts Bounty on Bugs*, CNET NEWS.COM, Aug. 2, 2004, *at* http://zdnet.com.com/2100-1105-5293659.html.

100 For a useful survey of self-help in American law, see Douglas Ivor Brandon et al., *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845 (1984) (examining role of self-help in self-defense, recovery of property, summary abatement of nuisance, resisting unlawful arrest and excessive force, liquidating damages, and repossessing property).

101 On vigilante justice in frontier settings, see ROBERT M. SENKEWICZ, VIGILANTES IN GOLD RUSH SAN FRANCISCO (1985).

fordable remedies,[102] and circumstances where potential offenders have proven to be indifferent to the effects of formal legal sanctions.[103]

This is not to suggest that we should accept uncritically the technological, legal, and moral claims of those who advocate the use of counterattacks against those who seek unauthorized access to property. After all, English jurists and Parliamentarians – who devoted roughly a decade to the subject – certainly had no such illusions. Despite the scourge of poachers, the weaknesses of formal law, the failures of "defensive" measures such as fencing and posting land, and the relative cost-effectiveness of spring guns, England's political leaders ultimately decided that private persons could not be trusted to operate spring guns in a socially responsible and socially optimal manner. Network security experts likewise operate in a world of persistent threats, imperfect policing, inadequate defenses, and high costs. But whereas spring guns proved to be "blind, unreasoning, undistinguishing, remorseless engines, [that] sacrificed every thing within their range,"[104] twenty-first century digital counterstrike technologies at least hold out the prospect of counterattacks that are clear-sighted, calculating, discriminating, and – if not remorseful – at least compensable.

---

102 For example, American landlords in the nineteenth century availed themselves of their right to evict tenants forcibly because civil actions for ejectment were costly, slow, and uncertain. Once American states adopted summary eviction statutes in the late-nineteenth century, the scope of a landlord's permissible self-help against holdover tenants was diminished. *See* JESSE DUKEMINIER & JAMES KRIER, PROPERTY 507-09 (5th ed. 2002).

103 Thus, John Lott has argued strenuously on behalf of gun ownership as a means of deterring would-be killers from committing murderous acts on the grounds that certain persons who commit homicidal acts seek to maximize the amount of damage they inflict and are indifferent to being punished themselves. *See* JOHN R. LOTT, JR., MORE GUNS, LESS CRIME: UNDERSTANDING CRIME AND GUN CONTROL LAWS (2d ed. 2000).

104 13 PARL. DEB. (2d ser.) 1257 (1826).

VIRTUAL CRIME, VIRTUAL DETERRENCE: A SKEPTICAL VIEW OF SELF-HELP, ARCHITECTURE, AND CIVIL LIABILITY

Orin S. Kerr[*]

Recent scholarship in the field of computer crime law reflects a surprising trend: much of it does not concern criminal law or the criminal justice system. According to many scholars, the problem of computer crime can be best addressed by looking beyond criminal law. Cybercrime demands a new model of law enforcement, the thinking goes; the traditional mechanisms of criminal investigation and prosecution cannot deter computer-related crime effectively.[1] The law must turn to alternative approaches that regulate social norms, code, and civil liability to alter incentives *ex ante* without recourse to the criminal justice system.[2]

This essay critiques three of the most prominent proposals to deter computer crime outside of criminal law. The first proposal, self-help, would allow victims of hacking and denial-of-service attacks to defend

---

* Associate Professor, George Washington University Law School. Thanks to Dan Hunter, Neal Katyal, Doug Lichtman, Dan Markel, Michael O'Neill, and Daniel Solove for their comments on an earlier draft. This essay was prepared for a symposium "Property Rights on the Frontier: The Economics of Self-Defense and Self-Help in Cyberspace" hosted by the *Journal of Law, Economics and Policy*. Thanks to Noah Falk for excellent research assistance, and to the editors of the *Journal of Law, Economics and Policy* for their gracious invitation to speak at the *Journal*'s first symposium.

[1] *See, e.g.*, Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L. J. 63 (2001) (arguing that "criminal law is an inadequate institution of social control against cybercrime," and that there is a "greater role for private 'cybercops' to punish and control cybercrime to close the enforcement gap"); Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 HARV. J. LAW & TECH. 699, 706-708 & fn. 14, 15 (1998) (discussing the need for public private partnerships in the deterrence of computer crimes); Susan W. Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security*, 10 B.U.J. SCI. & TECH. L. 1 (2004) (arguing that cybercrime demands a new model of law enforcement); Nimrod Kozlovski, *Designing Accountable Online Policing*, *available at* http://islandia.law.yale.edu/isp/digital%20cops/papers/kozlovski_paper.pdf ("The online crime scene introduces complex challenges to law enforcement that inevitably lead to the emergence of a new policing model . . . derive[d] from employing alternative strategies of law enforcement."); AMITAI AVIRAM, *Network Responses to Network Threats: The Evolution Into Private Cyber-Security Associations*, in THE LAW & ECONOMICS OF CYBER-SECURITY (Cambridge University Press; forthcoming 2005); Brent Wible, Note, *A Site Where Hackers Are Welcome: Using Hack-in Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L.J. 1577, 1577 (2003) ("With the failure of traditional law enforcement methods to deal with [the threat of computer crime], computer crime requires a new approach to thinking about deterrence."). *See also infra* notes 3-5.

[2] *See infra* notes 3-5.

themselves by counterattacking and disabling intruders.[3] The concept animating offensive self-help or "hack back" proposals is that private parties may be able to deter and prevent computer crimes through private action more effectively and efficiently than through government action. The second proposal, architecture regulation, was offered recently in an essay by Professor Neal Katyal.[4] Professor Katyal contends that computer crime can be deterred by redesigning the architecture of cyberspace in ways that mirror how architects design physical spaces to deter traditional crime. The third proposal, civil liability, seeks to impose liability on third-party intermediaries such as ISPs for the cost of criminal activity.[5] Although many variations of this proposal exist, my specific interest is on the use of civil liability to encourage ISPs to monitor and deter crime attempted by their subscribers.

This essay offers a skeptical view of the three proposals. I agree that responses to computer crime must look at least in part beyond criminal law. Criminal law addresses only a small piece of the broader puzzle of how to deter misconduct, and that is just as true online as it is offline.[6] At the same

---

[3] *See* Michael E. O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237 (2000); Curtis E. A. Karnow, *Launch on Warning - Aggressive Defense of Computer Systems*, *available at* http://islandia.law.yale.edu/isp/digital%20cops/papers/karnow_newcops.pdf; Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171 (2000); Bruce Smith, *Hacking, Poaching, and Counterattacking*, 1 J.L. ECON. & POL'Y (forthcoming 2005). *Cf.* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207 (2002) (discussing self-help measures under the rules of war).

[4] Neal Kumar Katyal, Essay, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261 (2003).

[5] *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, SUP. CT. ECON. REV. (forthcoming 2005); Assaf Hamdani, *Who is Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002); Stephen E. Henderson & Matthew E. Yarborough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N. M.L. REV. 11 (2002); Rustad, *supra* note 1; Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1009 (2001); Calkins, *supra* note 3, at 219-224; Robin A. Brooks, Note, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?*, 17 REV. LITIG. 343 (1998); David L. Gripman, Comment, *The Doors Are Locked but the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMP. & INFO. L. 167 (1997); Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213 (1995); Susan C. Lyman, *Civil Remedies for the Victims of Computer Viruses*, 21 SW. U.L. REV. 1169, 1172 (1992); Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167, 185 (1990); Anne Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 30-37 (1990); Agranoff, *Curb on Technology: Liability for Failure to Protect Computerized Data Against Unauthorized Access*, 5 SANTA CLARA COMPUTER & HIGH TECH. L.J. 263, 268 (1989).

[6] In the case of traditional crimes, no one would think to argue that criminal law should be the *only* mechanism to prevent crime. No one keeps their doors unlocked at night in the hope that burglars will break in, get caught, and then be prosecuted so as to deter future burglary attempts. Instead, we lock our doors. Conversely, few would argue seriously that there should be no criminal punishment at

time, the three proposals reflect in varying degrees a common conceptual mistake: over reliance on the metaphor of the Internet as a virtual "place." The proposals tend to envision the Internet as a virtual world of cyberspace with virtual streets and virtual management, and use this virtual model to generate assumptions about what kind of legal rules and practices are likely to generate particular results. These assumptions are valid in some circumstances, but they are not valid in many others. As a result, heavy reliance on virtual metaphors risks incorporating assumptions from the physical world that break down when applied to the Internet. When this occurs, virtual metaphors will obscure rather than illuminate the dynamics of computer crime.

This essay argues that responding to computer crime requires confronting the physical reality of what the Internet is and how it works. Both virtual and physical perspectives of the Internet can offer important lessons, but any strategy to deter computer crime must look viable given the physical reality of the network. Strategies that rely too heavily on the virtual metaphors of cyberspace are likely to rely on assumptions drawn from the physical world that do not apply to the Internet; the process of importing concepts from physical space to the virtual world of cyberspace will introduce errors. Over reliance on virtual metaphors will often misrepresent how online crime occurs and thus how it can be deterred. Where virtual metaphors govern, proposals to deter computer crime through civil liability and social norms will prove less effective in practice than they may first appear in theory.

I begin my argument by exploring the tension within Internet law between modeling the Internet using virtual reality and physical reality, with a special emphasis on what this tension means for developing arguments about deterrence and computer crime. The analysis explains that a physical description of the Internet differs dramatically from a virtual description of Internet applications, and argues that any effective model for deterring computer crime must be rooted in the former rather than the latter. In the remaining parts of the paper, I apply this insight to critique the three proposals. I begin with offensive self-help, focusing on Michael O'Neill's article *Old Crime in New Bottles: Sanctioning Cybercrime*; turn next to architecture regulation, focusing on Neal Katyal's essay *Digital Architecture as Crime Control*; and conclude by studying proposals that would impose civil liability on third-party computer operators. In each case, I identify how over reliance on virtual metaphors can frustrate efforts to deter computer crime.

---

all for burglary. We recognize that the criminal justice system offers a marginal deterrent value against burglary and serves important retributive ends as well. The basic regulatory strategy is to combine criminal law with other mechanisms to best deter crime while minimizing other social costs. I submit that this basic approach will likely prove the most effective strategy to deter and punish computer crime, as well.

I. PHYSICAL AND VIRTUAL APPROACHES TO DETERRING COMPUTER CRIME

There are two basic ways to model the Internet: from the perspective of physical reality and the perspective of virtual reality.[7] From a virtual perspective, the Internet can be understood as the home of a virtual world of cyberspace that is roughly analogous to the physical world. A user can utilize his keyboard and mouse to go shopping, participate in online communities, and do anything else that he finds online much like he could in the physical world. The Internet is cyberspace, a virtual world with virtual streets and virtual stores, virtual perils and virtual promise that echo the physical world.[8] The physical perspective of the Internet is very different. From a physical perspective, "the Internet" is a name attached to the sprawling and decentralized international network of networks including millions of computer servers and hundreds of millions of miles of cables. The hardware sends, stores, and receives trillions of digits of data every day using a series of common protocols. Many of the computers connected to this network of networks are located outside the United States, along with the majority of its users. Keyboards provide sources of input to the network, and monitors provide destinations for output. From the standpoint of physical reality, the virtual world of cyberspace is just a convenient metaphor. Internet users may decide to use that metaphor to more easily understand particular software applications available via the Internet. But what matters is the physical reality of the network, the actual bits and bytes, rather than the virtual world a user might imagine.

Understanding the distinction between physical and virtual descriptions of the Internet is critical to understand how law can help deter computer crime. The distinction between physical and virtual leads to two basic approaches to deterring cybercrime. From a virtual perspective, the natural starting point for regulating cyberspace is to translate the ways that the law regulates the physical world. If a problem from the physical world carries over into cyberspace, the solution from physical space should be harnessed, modified as necessary, and then applied to cyberspace. In the specific context of computer crime, the virtual perspective suggests that legislatures should study crime prevention strategies that have worked in physical space, and apply a virtual version of that solution to cyberspace. In a sense, computer crime is nothing new: it's just a cyberspace version of old-fashioned physical crime. The switch from physical to virtual may create

---

[7] *See generally* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91, GEO. L.J. 357 (2003).

[8] *Cf.* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 524 (2003) ("Even if we understand somewhere in the back of our minds that we are not really going anywhere, perhaps when we access the Internet it seems so much like we are in a different physical space that we accept cyberspace as a "real" or physical place.").

some new wrinkles, but the basic problem can draw from solutions already applied in the physical world.

From a physical perspective, computer crime is a different problem and calls for different solutions than you might see from a virtual perspective. The physical perspective teaches that online crimes involve users sending and receiving data in ways that the law seeks to prohibit. Perhaps the data is contraband, such as an image of child pornography. Perhaps the law prohibits the transmission or use of data because particular data is private and belongs to some one else, such as private files exposed by a hacker. Perhaps the data is copyrighted and cannot be distributed without permission. Or perhaps the transmission of data blocks others from being able to access their computers, such as might occur with a denial of service attack. In all of these cases, computer crime law attempts to regulate the transmission of data to avoid identified social harms. To deter computer crime, solutions either must block the transmission by code-based restrictions or else persuade users not to act in ways the law recognizes as harmful.

The distinction between physical and virtual is critical because solutions that appear promising from a virtual perspective might not appear promising from a physical perspective, and vice versa. Consider the example of "broken windows" policing.[9] In the physical world, individuals considering whether to engage in criminal activity often take clues from their physical environment.[10] Visible disorder can undermine law-abiding norms.[11] Tolerance of low-level criminal activity in a neighborhood can signal tolerance of higher-level activity, and may lead to more serious crime. "Broken windows" policing attempts to reverse that process. The visible enforcement of low-level activity signals to wrongdoers that higher level activity will not be tolerated; the hope is that perception of obedience to the law based on observable enforcement of the law helps generate norms of obedience and discourages crime.[12]

Does broken windows policing teach us anything useful about deterring computer crime? From the virtual perspective, the answer might appear to be "yes." Enforcement policies might place a priority on fixing broken "cyber windows," if you will, encouraging the visible enforcement of the law in one region of cyberspace to help generate norms of obedience to law in that region. Visible signs that the law is enforced in one cy-

---

[9] *See generally* GEORGE L. KELLING & CATHERINE M. COLES, FIXING BROKEN WINDOWS: RESTORING ORDER AND REDUCING CRIME IN OUR COMMUNITIES (1996).

[10] *See generally* Robert J. Sampson & Jacqueline Cohen, *Deterrent Effects of the Police on Crime: A Replication and Theoretical Extension*, 22 LAW & SOC'Y REV. 163 (1988).

[11] Dan M. Kahan, *A Colloquium on Community Policing: Reciprocity, Collective Action, and Community Policing*, 90 CAL. L. REV. 1513, 1527-30 (2002).

[12] *See id. But see* BERNARD E. HARCOURT, ILLUSION OF ORDER: THE FALSE PROMISE OF BROKEN WINDOWS POLICING (2001).

berneighborhood might send signals to cybercriminals that they should look elsewhere. From a virtual perspective, it seems plausible to look for ways to signal to potential cybercriminals that the cyber-community will not tolerate criminal activity in a particular corner of cyberspace.[13]

From a physical perspective, however, the answer appears to be "no." The notion of fixing windows in cyberspace makes little sense. Cyberspace is just a metaphor, not an actual place. Applying real-space approaches to "cyberspace" works only if the way that the approach applies to physical space happens to be replicated within the metaphorical understanding of cyberspace. This does not seem to occur in the case of broken windows policing. In the physical world, broken windows policing may work because there is an observable correlation between the visual appearance of a place and whether crime will be tolerated there. Visual appearance communicates information about law enforcement practices, and a potential wrongdoer can factor that into his decision whether to commit an offense.

The same linkage does not apply online. The visual appearance of a "site" on the Internet is merely a string of zeros and ones that the computer has been programmed to send to the user for reassembly and display. The string of zeros and ones does not reflect the social practices, priorities, or condition of the computer or its users. Whether the police pay attention to low-level criminal activity generally will not change the visual appearance of anything. Even if it did, the appearance of a site is known by wrongdoers to be merely a graphic overlay, not a signal of social norms or law enforcement practices. The homepage of a webserver looks the same regardless of whether the server is secure or is riddled with holes. Online intruders get a sense of the security practices used at a potential victim computer not by viewing the homepage of its webserver, but by remotely scanning the computer to determine its software, open ports, and vulnerabilities.[14] The dynamic underlying "broken windows" policing does not seem to apply to crimes involving the transmission of data from computer to computer. As a result, the strategy has little relevance in the context of computer crimes.

This example points to broader lesson about the role of physical and virtual perspectives in the formulation of cybercrime deterrence strategies. While both virtual and physical perspectives of the Internet can offer important lessons, any strategy to deter computer crime must look viable from a physical perspective. Strategies that rely too heavily on the virtual perspective of the Internet are likely to rely on assumptions drawn from the physical world that do not apply to the Internet. The process of importing

---

[13] *See* Katyal, *supra* note 5, at 1110 (suggesting that an application of the complementarity of crime underlying broken windows policing should lead to the swift and harsh punishment of computer virus authors to avoid copycat crimes).

[14] *See* Ofir Arkin, *Network Scanning Techniques: Understanding How It Is Done, available at* http://www.totse.com/en/hack/introduction_to_hacking/162026.html.

concepts from physical space to the virtual world of cyberspace risks importing too much. It threatens to let virtual metaphors get the best of us, and may point us in directions that do not actually work given the physical reality of the Internet. To ensure effective deterrence, care must be taken to make sure that no unwarranted assumptions are embedded in those strategies when they are transferred to the Internet.

This does not mean that metaphors are never useful, of course.[15] Metaphors harness existing similarities. When a new problem is similar in a relevant way to an old one, metaphors can illuminate how solutions from the old problem might apply to the new. The difficulty arises when one set of similarities generates a metaphor, and the metaphor is then used in other contexts where no relevant similarities exist. Consider e-mail and traditional postal letters. As a communications mechanism, e-mail is akin to traditional postal mail: e-mail is used to send and receive messages much like postal mail. When evaluating legal rules to regulate postal mail as a communications mechanism, it makes sense to invoke the virtual metaphor and begin by considering the legal rules used to regulate postal mail.

But this doesn't mean that snail mail and e-mail always should be treated alike. The fact that they are similar in some ways does not mean that they are identical in every way. For example, the existence of the United States Postal Service to deliver physical letters does not mean a centralized virtual Postal Service is needed to deliver e-mail. The fact that stamps are required to send postal mail doesn't mean stamps are needed to send e-mail. While postal letters and e-mail are alike in some ways, their delivery mechanisms are quite different. We cannot simply declare e-mail the virtual equivalent of physical mail and assume that every legal regulation of the latter should apply to the former. A more nuanced approach is required that looks carefully at the specific ways in which virtual and physical are similar and different.

The remainder of this essay will apply this critique to three sets of proposals that would attempt to deter computer crime outside of criminal law. I will begin with offensive self-help strategies, turn next to architecture regulation, and finish with civil liability for third-party computer operators. In each case, I argue that over reliance on the cyberspace metaphor weakens the analytical framework of the proposals. Excessive use of virtual metaphors creates unwarranted assumptions, and unwarranted assumptions leads to misunderstandings of how the law can deter computer crime.

---

[15] *See generally* Kerr, *supra* note 7, at 389-405 (offering a normative framework for when law should adopt a virtual versus a physical perspective of computers and the Internet).

II. OFFENSIVE SELF-HELP

Should the law permit victims of computer hacking attacks to counter-attack and disable intruders? A number of scholars have suggested that the answer is yes.[16] Professor Michael O'Neill has developed the most prominent proposal.[17] According to Professor O'Neill, traditional mechanisms of criminal investigation and prosecution do not sufficiently deter crime involving the Internet: there are too few cybercops, cybercriminals are too hard to catch, and jurisdictional hurdles often get in the way.[18] As an alternative, O'Neill proposes a regime of offensive self-help, or cyber-vigilantism. Allow victims of computer crimes to hack-back against those that hacked them. The threat of being hacked back will deter the initial round of hacking, O'Neill contends: potential attackers will know that an attack may lead to them being made the next victims, resulting in deterrence akin to a cyber-version of mutual assured destruction.

Professor O'Neill relies explicitly on virtual metaphors to explain and justify his proposal. He writes: "[J]ust as settlers in the American West could not reliably count on the local sheriff to protect them, and instead kept a weapon handy to stymie potential aggressors, Internet users may need to protect themselves."[19] "[C]yberspace is our new frontier,"[20] he adds, and private companies have the virtual firepower to keep "virtual streets"[21] safe. "Just as a homeowner may defend his house, . . . computer companies ought to not only be permitted, but encouraged, to unleash their considerable talents to launch countermeasures against cyber-criminals."[22] O'Neill appears to envision the Internet as a virtual Wild West, with cyber-settlers carrying virtual guns and mounting cyberdefenses against virtual bandits. Just as packing a weapon in the Wild West might deter wrongdoers, so can the threat of a cyberattack deter wrongdoers in cyberspace.

The image is a memorable one, but note the assumption embedded in the virtual metaphor. Use of the virtual metaphor presumes that victims of an attack can find out easily who is attacking them. This was often true in the Wild West, or at least in movies about the Wild West. If Bad Guy wants to attack Good Guy with a six-shooter, he needs to be close enough to see him and have a good chance of hitting him. At that very short dis-

---

16 *See supra* note 3. There is a great deal of commentary on a related question of whether the law should allow similar self-help measures by copyright owners to disable computer-facilitated copyright infringement. For the sake of simplicity, however, I will limit my discussion to self-help designed to prevent and deter unauthorized access to computers.

17 *See* O'Neill, *supra* note 3.

18 *See id.* at 275-77.

19 *Id.* at 277.

20 *Id.* at 279.

21 *Id.*

22 *Id.* at 280.

tance, Good Guy can see Bad Guy, too. If Good Guy has the same gun that Bad Guy has and there is no element of surprise, Good Guy and Bad Guy are on equal footing. My sense is that Professor O'Neill's proposal presupposes such a dynamic. Let's assume that Bad Guy is a rational actor. He will decide to kill Bad Guy if the benefit from attacking good guy exceeds the harm to himself. To throw in some unnecessary math, we can say that Bad Guy will attack when

> (Chance initial attack will succeed) * (Benefit to Bad Guy if initial attack succeeds) > (Chance Good guy will attempt a counterattack) * (chance counterattack will succeed) * (harm to Bad Guy if counterattack succeeds)

My sense is that O'Neill assumes that the chance that the counter attack will succeed is on par with the chance that the initial attack will succeed. The deterrence dynamic O'Neill seeks to harness is based on a type of ricochet effect; the likelihood that an attack will lead to a successful counterattack deters the initial attack.

Applying this regime to the Internet creates a significant problem, however. It is very easy to disguise the source of an Internet attack. Internet packets do not indicate their original source. Rather, they indicate the source of their most immediate hop. Imagine I have an account from computer *A*, and that I want to attack computer *D*. I will direct my attack from computer *A* to computer *B*, from *B* to computer *C*, and from *C* to computer *D*. The victim at computer *D* will have no idea that the attack is originating at *A*. He will see an attack coming from computer *C*. Further, the use of a proxy server or anonymizer can easily disguise the actual source of attack. These services route traffic for other computers, and make it appear to a downstream victim as if the attack were coming from a different source.

As a result, the chance that a victim of a cyber attack can quickly and accurately identify where the attack originates is quite small. By corollary, the chance that an initial attacker would be identified by his victim and could be attacked back successfully is also quite small. Further, if the law actually encouraged victims of computer crime to attack back at their attackers, it would create an obvious incentive for attackers to be extra careful to disguise their location or use someone else's computer to launch the attack. In this environment, rules encouraging offensive self-help will not deter online attacks. A reasonably knowledgeable cracker can be confident that he can attack all day with little chance of being hit back. The assumption that an attacker can be identified and targeted may have been true in the Wild West, but tends not to be true for an Internet attack.

Legalizing self-help would also encourage foul play designed to harness the new privileges. One possibility is the bankshot attack: If I want a computer to be attacked, I can route attacks through that one computer towards a series of victims, and then wait for the victims to attack back at that computer because they believe the computer is the source of the attack. By

harnessing the ability to disguise the origin of attack, a wrongdoer can get one innocent party to attack another. Indeed, any wrongdoer can act as a catalyst to a chain reaction of hacking back and forth among innocent parties. Imagine that I don't like two businesses, *A* and *B*. I can launch a denial-of-service attack at the computers of *A* disguised to look like it originates from the computers at *B*. The incentives of self-help will do the rest. *A* will defend itself by launching a counterattack at *B*'s computers. *B*, thinking it is under attack from *A*, will then launch an attack back at *A*. *A* will respond back at *B*; *B* back at *A*; and so on. As these examples suggest, basing a self-help strategy on the virtual model of the Wild West does not reflect a realistic picture of the Internet. Self-help in cyberspace would almost certainly lead to more computer misuse, not less.

To be fair, it is possible to generate a self-help proposal that does not rely on virtual metaphors. A proponent of the idea could restate it using physical rather than virtual descriptions of the Internet. In my experience, however, the persuasiveness of the self-help argument draws heavily on the virtual metaphor. The model of an online counterattack as a "virtual punch" or "virtual bullet" situates the proposal in a familiar physical setting, and supports the necessary but false assumption that an online victim can successfully disable his attacker much like a physical victim can disable a physical attacker. The virtual model incorporates assumptions that hold in the physical world but tends to hide the very different dynamics at work in the case of Internet attacks.

III. ARCHITECTURE REGULATION

Over reliance on virtual metaphors also blunts the effectiveness of architectural approaches to computer crime. In an interesting essay entitled *Digital Architecture as Crime Control,* Professor Neal Katyal contends that one answer to the problem of computer crime is to apply realspace notions of architecture regulation to cyberspace.[23] Katyal reasons that the "metaphorical synergy" between physical space and cyberspace justifies "a new generation of work" in which scholars apply "the lessons of realspace study . . . to the cybernetic realm."[24] Professor Katyal notes that in the physical world, architects can help deter crime by designing open and well-lit spaces,[25] by fostering notions of terroritoriality that signal stewardship of property,[26] and by fostering a sense of community.[27] Katyal proposes "reverse-engineering the realspace analysis of architecture . . . to cyber-

---

23 Katyal, *supra* note 4.

24 *Id.* at 2261.

25 *Id.* at 2264-67.

26 *See id.* at 2268-72.

27 *See id.* at 2272-79.

space"[28] to "help develop the types of digital bricks and mortar that can both reduce crime and build community" online.[29] If architecture regulation helps prevent crime in physical space, Katyal suggests, it also can help prevent crime in cyberspace.

Katyal relies heavily on virtual metaphors to frame his proposals. He suggests that the very idea of distinguishing between real space and cyberspace has a limited future: "the divide between realspace and cyberspace [is] erod[ing],"[30] Katyal contends. "With wireless networking, omnipresent cameras, and ubiquitous access to data, these two realms are heading toward merger."[31] According to Professor Katyal, architectural concepts "offer a vantage point from which to view this coming collision"[32] between real space and cyberspace.

But does the architectural approach shed light on deterring computer crime? An important difficulty lurks within Katyal's approach. Architecture can deter crime in physical space because architecture defines the properties of the space. Physical space follows immutable rules of physics; by changing the space, architects can change the likelihood that an attempted criminal act in that space will succeed and communicate that to potential perpetrators of criminal activity *ex ante*. Cyberspace is only a metaphor, however. It offers a way to understand the experience of using some Internet applications, but does not create an environment with a universal set of rules that govern all interactions with particular people or things. Any perception of "cyberspace" generally rests on a superficial visual facade over the real network, and a typical cybercriminal will be focused on the real network rather than the facade.

The fact that cyberspace is only a metaphor makes it difficult for architectural insights to advance the debate over strategies to deter computer crime. Users' impressions of the virtual metaphor play little to no role in their decisions to engage in misconduct. In all but a few cases, a potential perpetrator of a computer crime does not enter a "space" that signals the likelihood that a crime would be detected, or that a crime would succeed.[33] Cybercriminals tend to focus on the physical perspective, not virtual ones. They want to hack the network to get the machine to send and receive the information they want. Their focus is code, not the visual overlay. As a result, efforts to deter crime by influencing users' perceptions of the properties of cyberspace will tend to have little effect on computer crime.

I think we can see these difficulties in Professor Katyal's attempt to explain why architectural insights should trigger a new generation of think-

---

28 *Id.* at 2288.

29 Katyal, *supra* note 4, at 2289.

30 *Id.* at 2262.

31 *Id.*

32 *Id.*

33 Internet chat rooms are one obvious exception.

ing about cybercrime deterrence. Although Katyal's proposals are described as architectural, most have only a tenuous connection to architectural concepts. The inherent difficulty of architecting a metaphor encourages attention to be focused elsewhere. Consider the case of "natural surveillance" design principles. In the physical world, architects can design spaces to be well-lit and open; this raises the chances of detection, raises the cost of crime, and therefore helps deter that crime. Katyal's attempt to apply this to cyberspace leads him to conclude that open source software is preferable to closed source software.[34] More people can see the code underlying open source programs, Katyal notes; the code is "open." According to Katyal, the principles of natural surveillance teach that greater exposure facilitates greater attention, and greater attention to code among computer security experts can lead to the identification and correction of security defects.[35] As a result, open source software should lead to more secure code than closed source software.

While it may be right that open source software tends to have fewer defects than closed source software – the technical community generally believes this, and I have no reason to disagree – this insight is not related to natural surveillance. Natural surveillance can be used to deter crime by fostering a sense among potential offenders that an attempted crime is unlikely to succeed; a space is "open" in the sense that it any conduct can be observed by other people who can report the crime. Natural surveillance increases the chance of detection, raising the cost of crime to the wrongdoer. Debates about open source software concern a different question. In those debates, the issue is how to create incentives for software designers to identify and correct security vulnerabilities. The goal is not to dissuade attempted wrongdoing based on fear of detection, but to make code impervious to attack when wrongdoing occurs. Software is "open" not in the sense of being visible to wrongdoers, but in the sense that programmers can obtain copies to review for defects. Despite the superficial connection between the two, natural surveillance principles do not appear to relate to or shed light on the open source debate.

A similar difficulty exists with Katyal's views of how notions of territoriality should impact Internet design. Katyal explains that real space architects can design space to foster a sense of territoriality and responsibility for enclosed and private regions. The use of archways and open gates can create a sense of ownership and private property that can encourage others to stay away.[36] By controlling how people perceive whether there are welcome in particular spaces, architecture can help determine the likelihood that crime will occur there. Katyal contends that cyberspace architects can apply this principle to the Internet by designing systems that facilitate

---

34 *See id.* at 2264-65.

35 *See id.*

36 *See* Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039, 1058-59 (2002).

traceability. He focuses on the strengths and limitations of different privacy rules and practices, ranging from logging IP addresses to allowing content owners to subpoena ISPs for subscriber information.

Whatever the merits of these different rules and practices, however, the connection between them and realspace notions of territoriality is indirect at best. Territoriality rests on the perception that a space is someone's property; traceability rests on the idea that it should be possible to connect an individual's conduct to their person. The former deals with shaping attitudes about ownership and property rights *ex ante*; the latter concerns investigating crime *ex post*. To be fair, the two share a common theme of responsibility. In addition, traceability *ex post* can create disincentives to commit crime *ex ante*. At the same time, the fact that territoriality can be used in realspace design does not appear to shed light on the complex tradeoffs among different privacy rules and practices.[37] The connection is too indirect for the former to generate useful insights about the latter.

Finally, Katyal's proposals on community building appear to suffer from the same difficulty. In physical space, architects can design space to facilitate easy interaction and encourage a sense of community and common identity. They can put houses close together, and use public parks as common meeting places. According to Katyal, applying this insight to the Internet suggests that we should embrace (within limits) the end-to-end principle of network design.[38] The end-to-end argument is that the brains of a network operation should be at the ends of the network, rather than the middle; the network should be open to all types of different traffic and let the applications at the end point figure out what to do with them.

Lawrence Lessig and Mark Lemley have argued powerfully that end-to-end design is an important part of the Internet's architecture, and that facilitating future innovation depends on it.[39] They explain that end-to-end design ensures that the network remains open to technological change because the network does not discriminate among old and new types of communications. Katyal contends that the interest in community building also

---

[37] This is not to say that territoriality is irrelevant. Code-based restrictions can create a sense of territoriality, and I have argued elsewhere that such restrictions should be used to draw the line between legality and illegality in the case of unauthorized access statutes. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

[38] The end-to-end principle has been latent in the design of the Internet since its inception but was first explored systematically by Jerome Saltzer, David Reed, and David Clark in 1981. *See* Jerome H. Saltzer, David P. Reed, and David D. Clark, *End-to-End Arguments in System Design*, Second International Conference on Distributed Computing Systems (April 8-10, 1981) pages 509-512.

[39] *See* Mark A. Lemley & Lawrence Lessig, *The End Of End-To-End: Preserving The Architecture Of The Internet In The Broadband Era*, 48 U.C.L.A. L. REV. 925, 930-33 (2001). *See also* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 120-22 (1st ed. 2001).

supports end-to-end design.[40] An architect of the Internet would want easy interaction and reciprocity among computers much like a traditional architect would value easy interaction and reciprocity among people in physical space.[41] Because end-to-end facilitates interoperability among programs, the architectural insights of community building suggest the need for end-to-end design.[42]

The difficulty with this analogy is that computers are not people, and the comparison rests on attributes that humans have but Internet applications don't. Reciprocity and interaction can deter crime in physical space because community building creates a notion of shared responsibility. Shared responsibility fosters a willingness to look out for and respond to criminal activity. Reciprocity and interaction among computers generally is a good thing, but it is not clear how it relates to deterrence. Computers do not feel responsibility; they only look out for crime if they are programmed to do so. If there is a connection between end-to-end design and deterring computer crime, it is left unexplained.

To be clear, I share many of Professor Katyal's instincts on the merits. I share his sense that open source has advantages over closed source software, his interest in accountability, and his general agreement with end-to-end design. But labels matter, I think, and in this context architectural labels appear to hide the key questions rather than expose them. The core difficulty is that if the architectural approach is applied uncritically, any proposal can be justified as the application of one or more architectural theories. Every proposal opens law or code to more scrutiny, less scrutiny, or both. Under the architectural approach, however, any proposal that opens law or code to more scrutiny and interaction can be justified as an application of natural surveillance or community building principles. Conversely, any proposal that leads to law or code being less scrutinized can be justified as an application of territoriality principles. The virtual metaphor of cyberspace architecture is too flexible to be of much help in the design of strategies to deter computer crime.

IV. THIRD-PARTY CIVIL LIABILITY

Over reliance on virtual metaphors also undergirds a number of proposals to impose civil liability on third-parties for the costs of criminal activity. Here my critique is relatively narrow and cautious, in part because the literature is extensive and diverse. Scholarly discussion of third-party civil liability for computer crime dates back to the 1970s, and the relevant

---

40 *See* Katyal, *Digital Architecture, supra* note 4, at 2272-73.

41 *See id.* at 2273 ("Generally speaking, both online and offline, open networks for communication and transportation promote growth, opportunity, and interconnectivity.").

42 *See id.*

body of work includes dozens of different proposals.[43] For the sake of simplicity, I will focus on just one subset of this literature: ISP liability for subscriber misconduct. In recent years, a number of scholars have explored whether Reinier Kraakman's insights about the benefits of third-party enforcement can be applied to ISPs.[44] ISPs may be better equipped to deter crime than public law enforcement, the thinking goes. ISPs can monitor their subscribers for signs that they are engaging in computer hacking or distributing viruses, and then disable the accounts or take other action to block the misconduct.[45] By imposing liability on ISPs for the wrongs of their subscribers, the law may be able to create incentives for ISPs to deter the subscribers' criminal activity.

My interest in these proposals concerns the assumptions they make about the powers and capacities of ISPs. The proposals tend to assume that ISPs can monitor and control their property much like a physical property owner can monitor and control physical property. In effect, each computer is like a small patch of cyberspace: its owner should be able to see what is going on in that area of cyberspace much like an employer can watch what is going on in the workplace. The owner can also control what he sees and take action to address problems and eliminate sources of wrongdoing. ISPs can act like chaperones at a high school dance, ferreting out untoward conduct and requiring the offenders to leave.[46] Or perhaps ISPs can develop hacker profiles of characteristic hacker activity; when an account is used in a way common to what a hacker would do, the ISP can study that account closely for signs of illegal activity.[47] The common theme is that computer owners can know and control what is happening within their networks; civil liability can lead to less crime because computer owners have the power (and, with civil liability, the incentive) to minimize criminal activity.

But is this assumption valid? There are good reasons to think the answer is "no." In the context of physical space, third-party monitoring generally refers to visual observation. Visual observation can provide a remarkably efficient surveillance tool to identify wrongdoing. A chaperone

---

[43] *See supra* note 5. For an early article on the role of civil liability see Susan Nycum, *Liability for Malfunction of a Computer Program*, 7 RUTGERS COMPUTER & TECH. L.J. 1, 1-22 (1979) (considering the prospect of civil liability for creators of software programs).

[44] *See* Reinier Kraakman, *Gatekeepers: The Anatomy of a Third Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 100-101 (1986). For applications of Kraakman's idea to ISP monitoring, *see, e.g.*, Katyal, *supra* note 5, at 1095-97; Hamdani, *supra* note 5, at 910-12; O'Neill, *supra* note 3, at 282-84.

[45] *See* Posner & Lichtman, *supra* note 5, at 18-20; Katyal, *supra* note 4 at 2284-85; O'Neill, *supra* note 3, at 282-84.

[46] *See* O'Neill, *supra* note 3, at 283-84. *See* Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1096.

[47] *See* Katyal, *supra* note 5, at 1096 ("ISPs could also develop sophisticated hacker profiles that permit them to survey large numbers of users and pick out those who look suspicious because they repeatedly try to enter certain sites.").

at a high school dance can look at the dancers and easily tell if they are acting inappropriately. Visual observation is powerful; our eyes are trained to identify subtle patterns and reach quick conclusions. When proponents of ISP liability discuss ISP monitoring, they tend to draw from our instinct that computer monitoring must be something like visual monitoring. The word "monitoring" generally is used in an abstract way to suggest a virtual form of visual observation.

The virtual metaphor papers over the technical details, however, and those technical details indicate important limitations on ISP abilities. When you look more carefully at the technical problems, a different picture of ISP abilities emerges. Most obviously, ISPs cannot actually "see" accounts. They can only monitor accounts in ways that computer code allows, and that monitoring typically involves some form of wiretapping. Consider rules of liability that would encourage ISPs to determine when a customer is engaging in wrongdoing. How can an ISP know what a customer is doing? The most obvious approach would be to wiretap the customer's account; the ISP could install a surveillance device that taps into and records the user's line of traffic. As a technical matter, however, it is quite difficult to go from a stream of Internet traffic to a conclusion that a particular person was responsible for particular conduct. The data stream does not tell you who is using the account, or in what context. The ISP may be able to identify whether a user's account sent out a particular piece of malicious code, but it lacks the ready means to identify who sent it, or whether it was sent knowingly or unknowingly.

Unless an ISP wants to devote a full-time employee to following the conduct of a few accounts – quite a costly proposition given that ISPs can have millions of customers – the most viable monitoring tactic is "dumb" monitoring that can only look for particular bits and bytes of known code or trends in usage. Dumb monitoring has a high error rate, however, and is relatively easy to defeat. Consider our experience with spam filters. Spam filters monitor and attempt to identify incoming spam in much the same way that an ISP might try to monitor outgoing communications to identify malicious code. As anyone with an e-mail account will attest, spam filters never work perfectly: they only detect a proportion of spam, and occasionally block mail that is not spam. Ease of circumvention is also critical. If a person knows his ISP is monitoring his outgoing traffic to look for malicious code, he can take simple steps to ensure that his code evades the monitoring. He can encrypt the code, or send it in parts, effectively defeating the ISP's filters. In short, comprehensive ISP monitoring appears to be extremely difficult, even putting aside the very important privacy questions it raises. ISPs can have hundreds of thousands or even millions of customers; it is very difficult and time consuming for an ISP to watch just one or two customers in a comprehensive way; and it is easy for any customer to circumvent or defeat ISP monitoring.

Even proposals not reliant on virtual metaphors can be weakened by lack of attention to technical detail, leading to an unwarranted confidence in ISP monitoring abilities. For example, Doug Lichtman and Eric Posner suggest that ISPs may be able to program their computers to create a profile for each user, and then regularly compare that profile to usage patterns.[48] They write:

> [An] ISP can detect criminal behavior by analyzing patterns of use, much as a bank can detect credit card theft by monitoring a customer's pattern of purchases. Some patterns of use are intrinsically suspicious, for instance a continuous stream of communications from a home user. Other patterns are suspicious because they represent a radical departure from the user's ordinary behavior. If an ISP programs its computers to create a profile for each user, and then regularly compares the user's current patterns with that historic profile, the ISP should be able to detect this genre of unauthorized usage and intervene.[49]

While this may sound promising at first, it is worth pointing out the major differences between credit card account monitoring and the kind of ISP monitoring Lichtman and Posner suggest. Credit cards are used to purchase goods and services, and sellers must be registered and report every purchase immediately. Patterns of misuse are easy to identify; a credit card thief typically will attempt to run up as many purchases as the card will handle before a purchase is rejected. An attempt to max out the card will invite suspicion, and it is easy to program a computer to detect when that attempt occurs.

But what are the similar patterns for detecting criminal behavior in the case of an Internet account? Computers connected to the Internet can be used in an infinite number of ways to do an infinite number of things. The diverse range of Internet applications and uses for them makes it difficult (if not impossible) to identify a reliable marker that correlates with criminal activity. Lichtman and Posner suggest that a continuous stream of communications from a home user could signal criminality. But a continuous stream of communications could mean many things. Perhaps the user is merely uploading a large file; perhaps he is using a peer-to-peer networks to distribute files (whether copyrighted or not); perhaps the user has installed software allowing his computer to host Internet relay chat channels; perhaps he is sending e-mails with very large attachments. The transfer of data from a home user does not correlate sufficiently closely with criminal activity to warrant ISP investigation.

These difficulties do not mean that civil liability on third-party providers is necessarily a bad idea. But I think they provide reason for caution. Before the law adopts such a strategy, care should be taken to ensure that they do not rest in part on assumptions carried over from physical world dynamics that may not apply to the Internet.

---

48 *See* Lichtman & Posner, *supra* note 5, at 18.

49 *Id.*

CONCLUSION

The cyberspace metaphor is a powerful tool. It provides insights that help us understand our online interactions and their social meaning. At the same time, reliance on the virtual metaphor of cyberspace carries considerable dangers. At its worst, the virtual metaphor blinds us to how the Internet works; it substitutes metaphors from physical space instead of the reality of the Internet's dynamics. Deterring computer crime requires more focus on the reality of the network and less on metaphors of virtual worlds. A focus on the physical perspective of the Internet can ensure that concepts of deterrence that sound plausible in theory are also realistic in practice.

HOW THE LAW RESPONDS TO SELF-HELP

Douglas Lichtman[*]

Legal rules are typically implemented through a combination of public and private mechanisms. Burglars, for example, are deterred from unauthorized entry in part by the threat of jail time and police intervention, and in part by the knowledge that homeowners have guns, security systems, and other private measures by which to defend their property. Similarly, while entrepreneurs obviously use patent, copyright, and trade secret law to protect proprietary information, they also routinely take matters into their own hands by, for example, dividing sensitive information across employees such that no single employee ever knows enough to betray the firm completely. Every area of law can to some degree be characterized in this manner, framed in a way that emphasizes substitutability between public responses and their private alternatives. In this Essay, I examine several specific areas of law from this perspective, using each as a case study from which to cull broader lessons about the proper structure for these public/private partnerships.

I begin in Part I with examples relating to the First Amendment. Because of the First Amendment, courts evaluating free speech restrictions strongly favor private mechanisms over public ones. Indeed, government speech restrictions are often held unconstitutional on the specific ground that the government failed to show why some privately administered self-help remedy was not equally effective, and hence constitutionally preferred. I draw on these cases to explore and in various ways challenge a basic intuition about the relationship between state-sponsored remedies and their self-help alternatives: namely, that the existence of a cost-effective self-help remedy argues against government regulation as a means to accomplish similar ends.

I turn in Part II to trade secret law, a legal regime that explicitly casts self-help as a prerequisite to more formal legal protections. That is, trade secret law offers protection only in cases where the relevant secret holder has already made reasonable private efforts to maintain the secret. I consider why trade secret law relies on self-help in this fashion, and why self-help is not more often required in other legal settings. I also examine the reasons why state-sponsored trade secret remedies are available at all, given

---

* Professor of Law, The University of Chicago. This Essay is based on my remarks at the symposium, "Property Rights on the Frontier: The Economics of Self-Help and Self-Defense in Cyberspace," which was hosted by George Mason University on September 10, 2004. For helpful comments, my thanks to conference participants, and also Douglas Baird, Will Baude, Tom Bell, Bob Bone, Mark Lemley, Saul Levmore, Tom Miles, Tony Reese, Geoff Stone, Lior Strahilevitz, and Adrian Vermeule.

that private parties do have self-help mechanisms by which to protect their own secrets and would use those mechanisms in a world where the government chose not to intervene.

In Part III, I focus on copyright law. More so than virtually any other area of the law, copyright is constantly being reshaped by self-help technologies. At the moment, powerful new tools for content duplication and distribution are attracting most of the attention, raising doubts over whether existing copyright protections can be meaningfully enforced. Tomorrow, however, advances in encryption technology could easily reverse that trend, empowering authors to control their works in ways that copyright law never imagined, and without any of the concessions that copyright law has always intended. I consider how copyright is responding to both of these realities, struggling to remain relevant in a world where formal legal remedies are often too slow to adapt to changing technological threats. I also focus on a particular legal rule that is somewhat unique to copyright: an equitable doctrine that might well force private parties to choose between public and private mechanisms, rather than allowing private parties to rely simultaneously on both.

In Part IV, I use patent law to consider a special subset of private remedies: remedies that are as a general matter illegal, but are permissible in specific circumstances. The most familiar example here is violence that is excused by the privilege in favor of self-defense. The logic is that police officers and other government officials cannot adequately protect citizens from certain types of imminent harm, and thus in those narrow cases citizens are allowed to engage in what would otherwise be criminal aggression. As I will explain, patent law offers its own fact patterns of this sort, and those fact patterns help to unravel the more general puzzle of when legal rules should tolerate otherwise-disfavored forms of self-help.

Finally, in Part V, I briefly conclude, tying my work here into the broader themes of the conference for which this Essay was first prepared.

I. CAPTIVE AUDIENCES AND THE FIRST AMENDMENT

The existence of cost-effective self-help remedies often argues against government regulation as a means to accomplish similar ends; and nowhere is that more apparent than in the vast jurisprudence that surrounds the First Amendment.[1] On countless occasions, courts have struck down government restrictions on speech for the simple reason that self-help provides a seem-

[1] Excellent discussions on the general topic of how self-help opportunities affect First Amendment jurisprudence include Douglas Ivor Brandon et al., *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845, 855-58 (1984); Tom W. Bell, *Free Speech, Strict Scrutiny, and Self-Help: How Technology Upgrades Constitutional Jurisprudence*, 87 MINN. L. REV. 743 (2003).

ingly adequate alternative. Thus, when the city of Los Angeles arrested a war protestor whose jacket bore the now-infamous "Fuck the Draft" inscription, the Supreme Court held the relevant ordinance unconstitutional. Offended viewers, the court explained, have a sufficient self-help remedy in the form of simply averting their eyes.[2] Similarly, in a long line of cases involving speakers caught advocating crime, sabotage, and other forms of violence as a means of achieving political or economic reform, the Court (albeit after a false start or two[3]) again struck down government restrictions, emphasizing that, where there is "time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence."[4]

This is of course not to imply that every self-help mechanism is favored. Violence, for example, can very effectively discourage speech, but violence is a form of self-help to which the government has no obligation to defer. Similarly, hecklers from time to time chill speech by hurling insults (and sometimes glass bottles) but again the government is not required in these instances to sit idly by.[5] That said, it is nevertheless striking how often courts invalidate government regulations simply because plausible self-help alternatives are available. The New York Public Service Commission was for this reason rebuked when it attempted to prohibit power companies under its jurisdiction from including with customer bills pamphlets discuss-

---

[2] *See* Cohen v. California, 403 U.S. 15, 21 (1971) ("Those in the Los Angeles courthouse could effectively avoid further bombardment of their sensibilities simply by averting their eyes.").

[3] *See, e.g.*, Abrams v. United States, 250 U.S. 616 (1919) (upholding convictions under facts like these over a dissent by Justice Homes that articulates what would become the dominant and more generous view).

[4] Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring). The quote ought not be taken too literally. For example, surely the touchstone is not "time"; in many instances, there will be no meaningful future opportunity to reach the tainted audience no matter how much time might pass, and in such cases additional speech would be an empty remedy. That caveat aside, the Court often invokes this idea of speech chasing speech. *See, e.g.*, Gertz v. Welch, 418 U.S. 323, 344 (1974) ("The first remedy of any victim of defamation is self-help—using available opportunities to contradict the lie or correct the error and thereby to minimize its adverse impact on reputation.").

[5] An interesting question is whether the government in extreme cases might even have an obligation to intervene on the speaker's behalf. *See, e.g.*, Cantwell v. Connecticut, 310 U.S. 296, 308 (1940) ("When clear and present danger of riot, disorder, interference with traffic upon the public streets, or other immediate threat to public safety, peace, or order appears, the power of the state to prevent or punish is obvious."); Feiner v. New York, 340 U.S. 315, 326 (1951) (Black, J., dissenting) ("I reject the implication of the Court's opinion that the police had no obligation to protect petitioner's constitutional right to talk . . . . [I]f, in the name of preserving order, they ever can interfere with a lawful public speaker, they first must make all reasonable efforts to protect him."); Elena Kagan, *Private Speech, Public Purpose: The Role of Governmental Motive in First Amendment Doctrine*, 63 U. CHI. L. REV. 413, 431-32 (1996) (questioning whether the government should be allowed to limit speech merely because other citizens react with hostility to it); GEOFFREY R. STONE ET AL., THE FIRST AMENDMENT 67-75 (1999) (discussing expression that provokes a hostile audience reaction and asking whether the First Amendment should require "the police to arrest hostile members of the audience rather than stop the speaker").

ing politically sensitive subjects like the use of nuclear energy.[6] The restriction was unconstitutional, said the Court, because offended customers have an adequate self-help response: they can throw any troubling pamphlets away. More recently, the federal government has repeatedly failed in its attempts to regulate indecency online, again because self-help—here in the form of software filters that empower Internet users to block speech at the receiving end rather than interfering with speech at its source—calls into question the government's assertions that the proposed regulations serve a compelling state interest, let alone are sufficiently tailored to pass constitutional muster.[7]

Two intuitions seem to animate these various decisions. First, self-help in these examples makes possible diverse, individuated judgments. It increases the flow of information by allowing willing speakers to reach willing listeners, and it at the same time empowers unwilling listeners to opt out of the communication at low cost. This is attractive because society has a strong interest in allowing each individual to decide for himself what speech to hear. There are of course caveats to this argument; as I will argue below, sometimes individual judgments should be trumped and listeners should be forced to consider information and confront viewpoints that they would rather avoid.[8] However, in most instances, deferring to the individual is attractive, and thus self-help is favored because it offers listeners significant flexibility to choose what they will hear and also what they will ignore.

---

[6] *See* Consolidated Edison Co. v. Public Serv. Comm'n, 447 U.S. 530, 542-44 (1980).

[7] *See* Reno v. ACLU, 521 U.S. 844, 879 (1997) (finding that the government failed to carry its burden of showing that self-help technologies "such as requiring that indecent material be 'tagged' in a way that facilitates parental control of material coming into their homes" would not be as effective as the challenged statute); Ashcroft v. ACLU, 124 S. Ct. 2783, 2792-93 (2004) (finding similarly that the government failed to carry its burden in showing that software filters were less effective than the challenged statute). The Court in these cases actually blurs two distinct arguments. One argument is that the existence of private remedies like filters should lead to the invalidation of any government regulation designed to accomplish the same ends. The other argument is that, because the government can subsidize filters or otherwise increase their efficacy, the government must opt for interventions of that sort, rather than trying to regulate indecency directly. Put differently—and as Tom Bell stresses in his work—self-help has implications for two aspects of First Amendment analysis: the question of whether the regulation in question serves a compelling state interest, and the question of whether a regulation that serves a compelling interest is sufficiently tailored. *See* Bell, *supra* note 1.

[8] *See infra* notes 16-25 and accompanying text. *Accord,* CASS SUNSTEIN, REPUBLIC.COM (2003) (worrying that the Internet makes it too easy for people to hear only what they want to hear). Interestingly, sometimes the best way to force individuals to be exposed to new ideas is to invalidate a government speech restriction and thereby force individuals to rely on self-help. The reason is that a government ban will in certain situations be more effective than the corresponding self-help mechanism. A policy that favors self-help therefore might on its face seem to promote individuation, but in practice force more people to be exposed to unwanted messages. Thus, if the goal is to expose people to diverse views, there is no single best approach. Sometimes that goal is better served by favoring self-help over direct regulation; other times that goal is better served by favoring direct regulation over self-help.

Second and perhaps more important, self-help in these examples reduces the government's overall role in regulating speech. The First Amendment is suspicious of government regulation not only because regulation inevitably brings with it the possibility that some manipulative government official will use a seemingly innocuous regulation to in fact advance a particular viewpoint—a classic First Amendment concern—but also because even well-intentioned regulations can, given the enormous influence of the state, inadvertently skew public discourse. The V-Chip offers a sharp example for this latter concern. The V-Chip is a government-facilitated technology that helps parents filter television content.[9] Television manufacturers are required to build the filter into every new model 13 inches or larger; and the filter works by reading ratings that are encoded onto broadcast television signals. Those ratings evaluate each program based on a scale that focuses primarily sexual content, language, and violence, and the scale thus makes it easy for parents to filter based on these characteristics. But (and here is the problem) the scale does nothing to help parents filter based on other characteristics, such as religious overtones or political content. The result is that parents who might have previously taken the time to help their children make educated choices based on a combination of all five factors might now opt for the easier approach of just focusing on the government-facilitated three. If that happens—an open question given how few families currently use the V-Chip—the government's intervention will have skewed content decisions: the importance of the favored characteristics will be amplified at the expense of characteristics not included in the official rating scheme.[10]

The V-Chip example is all the more troubling because the content skew I describe here was not inevitable. Suppose, for example, that the V-Chip were designed not to filter based on specific predetermined characteristics, but instead to filter using collaborative filtering techniques. My family would identify fifteen programs that we deem appropriate. The collaborative filter would use those choices to identify other families with similar tastes. Then the filter would use the choices made by those other families to make recommendations to my family, and it would use future choices made by my family to make recommendations to those other families.

---

[9] *See generally*, Jack M. Balkin, *Media Filters, The V-Chip, and the Foundations of Broadcast Regulation*, 45 DUKE L. J. 1131 (1996). The government is as a technical matter responsible for only part of the V-Chip rating system; the rest the broadcast industry developed on a "voluntary" basis. As Balkin explains, however, the reality is that the government put extraordinary pressure on broadcasters to implement this filtering regime and in fact still today oversees many of the relevant details. In the text, I therefore intentionally describe the V-Chip as a form of government regulation, even though government officials would very much resist that description.

[10] Jack Balkin sounded this alarm right after the V-Chip was first introduced. *See* Balkin, *supra* note 9, at 1166 ("Filtering mechanisms are not neutral means of organization, blocking, and selection. They have important effects on what kinds of materials are subsequently produced and how social arrangements are subsequently organized.").

Never would any of us need to be explicit about what characteristics drive us to disapprove of one program while favoring another. And, rather than being limited to choose based on the government's three characteristics, our pattern of choices might naturally result from a complicated balance of hundreds of different characteristics, namely ones on which we and like-minded families implicitly agree. The government-imposed skew inherent in the current system would be removed; and the very same First Amendment interests championed by self-help in my original examples—individuation, and a reduction in the chance that government regulation will intentionally or inadvertently favor one perspective or subject over another—would at the same time be vindicated.[11]

These two touchstones—individuation, and a reduction in government involvement—do more than help to identify cases where self-help might offer an attractive alternative to government regulation; they also help to identify types of self-help that ought to be disfavored. Heckling, for example, drowns out and discourages speech that otherwise might have been warmly received by a willing audience. It is therefore unattractive on grounds of individuation. Violence similarly is an obstacle to individuation in that it allows a subset of the audience to impose its will on the remainder. With respect to government involvement, meanwhile, violence and extreme forms of heckling both actually increase the need for government intervention. They do so by creating situations where the government must step in to protect public safety.

Courts sometimes insert a third consideration into the mix: the notion that self-help should be preferred only in instances where it will be "equally effective" in terms of achieving the objective that the government regulation itself would target.[12] I do not embrace this third consideration because,

---

[11] Another approach would have been to require that the V-Chip be accessible to alternative rating systems, including ones that might have chosen to emphasize factors other than sex, language, and violence. This was actually proposed during the rule-making proceedings at the Federal Communications Commission, but the idea was rejected over concerns about costs and complications. *See* In re Technical Requirements to Enable Blocking of Video Programming Based on Program Ratings, 13 FED. COMM. REC. 11248 (1998) at ¶11 ("Although we are not mandating that TV receiver manufacturers provide for alternative rating systems, we encourage manufacturers to design TV receivers to provide for additional rating systems to the extent practical."). Competing rating systems are used for Internet filtering, although a small number of systems seem to dominate. *See* Fernando A. Bohorquez, Jr., *The Price of PICS: The Privatization of Internet Censorship*, 43 N.Y.L. SCH. L. REV. 523, 529-31 (1999) (discussing competing rating systems for online content).

[12] The Tenth Circuit made this mistake when it defended the federal Do-Not-Call registry on the ground that caller ID is not "an equally effective alternative" for minimizing the intrusion caused by unwanted commercial solicitations. *See* Mainstream Marketing Service, Inc. v. FTC, 358 F.3d 1228, 1245 (10th Cir.), *cert. denied* 125 S. Ct. 47 (2004). Such a statement is likely true—as the panel noted, widespread reliance on some form of caller ID would trigger a "technological arms race" with consumers working to screen calls more effectively and the telemarketing industry striving to defeat those protections with various technological masks—but that statement resolves nothing, as the question

in my view, the First Amendment at the very least must represent a commitment to sacrifice some modicum of efficacy in order to reduce government involvement in speech regulation. Besides, assertions along these lines are squarely inconsistent with the facts of the foundational cases. The option of averting one's eyes to avoid exposure to an offensive message, for example, is not as protective as a government intervention that would forbid the dissemination of such messages in the first place. The unwilling audience member will typically have to confront at least a glimpse of the offensive message before knowing to turn away, and the process of watching for offensive messages itself necessarily reminds unwilling audience members of exactly the communications they were hoping in the first place to avoid. Similarly, fighting speech with speech is certainly not as effective as prohibiting the troubling speech ex ante, among other reasons because speech in rebuttal rarely garners as much attention as the more sensational speech to which it is designed to respond.[13] As Eugene Volokh has previously noted, to claim otherwise in any of these cases is to unfairly impugn the motives and competency of the relevant lawmakers, in essence accusing them of indefensibly opting for law when self-help would have done just as well.[14] Worse, these assertions hide an important step in First Amendment analysis: comparing the loss in efficacy to the gains associated with removing a formal government regulation on speech.[15]

My examples thus far all explore this intuition that, in the context of the First Amendment, the *existence* of a plausible self-help remedy poses a

---

before the court was not whether self-help was a strictly better approach, but instead whether its deficiencies were so great as to justify a type of government regulation that is constitutionally disfavored.

[13] *See* Gertz v. Welch, 418 U.S. at 344 n.9 ("Of course, an opportunity for rebuttal seldom suffices to undo the harm of defamatory falsehood. Indeed the law of defamation is rooted in our experience that the truth rarely catches up with a lie.").

[14] Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1997 SUP. CT. REV. 141, 156.

[15] The loss in efficacy is the primary cost associated with self-help in these First Amendment examples, but there is another cost that must be accounted for as well: a system that relies on self-help rather than direct government intervention will often favor the wealthy and informed over those with fewer resources or less information. Software filters, for example, can help Internet subscribers avoid indecency online, but they are expensive to acquire and must be installed and maintained by a knowledgeable party. The Supreme Court decision in *Ashcroft* thus has an unequal impact: families with the resources to effectively wield filters might indeed have a plausible alternative to the statute struck down in that decision, but families without those resources as a practical matter do not. *See* Ashcroft v. ACLU, 124 S.Ct. 2783 (2004). Many families fall into that latter category: families where the children are more adept at disabling the filter than parents are at securing it; families where the parents lack the time and knowledge to install and monitor a filter but would obviously benefit from any automatic protection put in place by a federal statute; and so on. *See id.* at 2802 (Breyer, J., dissenting) (objecting to filters for these reasons). It is admittedly unclear how far to take this argument, however, given that wealth effects pervade every solution. Government regulation, for example, likely favors the wealthy, given that wealth surely buys influence over the legislative and regulatory process, let alone facilitating access to courts and other enforcement mechanisms.

challenge to the government's claim that direct intervention is required. But in First Amendment jurisprudence the opposite argument also plays a prominent role: where a "captive audience" has no effective self-help mechanism by which to avoid exposure to a given communication, that absence of a plausible self-help mechanism is taken to be an argument in favor of direct government regulation.[16] The point was perhaps most famously made in *Cohen v. California*, the case I mentioned earlier involving the offensive anti-war jacket. The city of Los Angeles defended the arrest in that case on the ground that, because citizens cannot avoid occasionally coming to the local courthouse for official business, and once in the courthouse they cannot avoid being exposed to communications originating around them, the city ought to be allowed to prohibit malicious speech within courthouse walls.[17] Captive citizens have no self-help options, argued Los Angeles city officials, and that lack of any plausible self-help alternative justifies a speech restriction that might otherwise not be permissible.

The captive audience argument was rejected in *Cohen*,[18] but the theory has been invoked in many other instances, and with varying degrees of success. For example, when the city of Shaker Heights, Ohio, decided to allow advertisements to be displayed inside its public transit system, four Justices emphasized audience captivity as an important factor in justifying a government restriction on the types of advertisements allowed,[19] and a fifth would have gone farther and on this argument banned advertisements entirely.[20] By contrast, when the city of Jacksonville, Florida, enacted an ordinance designed to stop drive-in movie theaters from displaying potentially offensive visuals in instances where the images would be visible from the

---

16 On this theory, the less a listener is able to defend himself from an unwanted message, the greater the government's interest in either facilitating self-help, or directly regulating the unwelcome speaker. To say that an audience is "captive" is thus to say that the costs of engaging in self-help are particularly high. *See* Bell, *supra* note 1, at 752 ("An audience qualifies as 'captive' only if it lacks attractive self-help remedies for countering offensive speech."). For a general introduction to the captive audience doctrine, see Geoffrey R. Stone, *Fora Americana: Speech in Public Places*, 1974 SUP. CT. REV. 233.

17 *Cohen*, 403 U.S. at 21-22.

18 The argument was rejected primarily because the statute at issue applied not only to disturbances where the captive audience argument has force—malicious speech disseminated in confined spaces like the courthouse—but also more broadly to any disturbance that would disrupt the "peace or quiet of any neighborhood or person." *See id.* at 22 (citing and discussing CAL. PENAL CODE § 415 (1971)).

19 Lehman v. Shaker Heights, 418 U.S. 298, 302-04 (1974).

20 *Id.* at 307-08 (Douglas, J., concurring) ("In my view the right of the commuters to be free from forced intrusions on their privacy precludes the city from transforming its vehicles of public transportation into forums for the dissemination of ideas upon this captive audience."). Interestingly, one wonders whether riders on public transportation are today meaningfully captive given the ubiquity of portable CD players, cellular telephones, and other technologies that afford a rider easy access to outside communications.

public streets, six Justices endorsed the view that the government can selectively "shield the public" in cases where "the degree of captivity makes it impractical for the unwilling viewer or auditor to avoid exposure,"[21] but the six then announced that in this particular situation the necessary degree of captivity was not realized because drivers could simply look away.[22] Personal residences are a setting where concerns about captivity have had particular bite, presumably on the rationale that citizens in their homes should have maximal protection from communications they might find offensive. Thus, in the leading case, the Federal Communications Commission was found to have acted within constitutional boundaries when it prohibited the use of certain vulgar words on the radio, both because "material presented over the airwaves confronts the citizen, not only in public, but also in the privacy of the home,"[23] and because home audiences are captive, with the only plausible self-help solutions being relatively unattractive options like changing the channel at the first sign of offense or refusing to listen to the radio at all.[24]

Important distinctions can be drawn between these several examples, in that they vary with respect to the nature of the speech at stake, the severity of the speech restriction being challenged, and the degree of audience captivity involved. Those details aside, however, the central insight here is that, where relevant at all, the existence of a captive audience is seen to argue exclusively in favor of government restrictions on speech. That is in my view a fundamental mistake. The absence of plausible self-help remedies is not merely a deficiency that the government ought to be allowed to address, but also an opportunity that the government ought not be allowed to without justification squander.

Think of it this way: we as a society have a strong interest in finding ways to ensure that each of us is exposed to a wide variety of conflicting perspectives. Society in fact expends significant social resources in pursuit of this goal, tolerating repulsive speech like that which originates with hate groups like the Ku Klux Klan; accommodating protesters even at abortion clinics where their message will inevitably upset already fragile emotions; requiring broadcasters to air programming devoted to education and news even though viewers would strongly prefer other television fare; limiting plausibly efficient industry consolidation in and across the radio, television, and newspaper industries for fear that consolidation might lead to confor-

---

21 Erznoznik v. Jacksonville, 422 U.S. 205, 209 (1975).

22 *Id.* at 212. This case differs along an important dimension from my earlier examples in that the owner of the drive-in had very little interest in exposing uninterested drivers to his films (perhaps only to the extent that short glimpses would serve as free advertising), whereas the speaker in *Cohen* was very much targeting a population that might be offended by, but forced to think about, his anti-war message.

23 FCC v. Pacifica, 438 U.S. 726, 748 (1978).

24 *Id.* at 748-49.

mity in thought or perspective; and, among many other examples, spending real tax dollars each election cycle to finance political campaigns, with much of that money ironically spent to attract the sort of voter attention that the captive audience would naturally provide.

Against this backdrop, audience captivity has genuine and unappreciated appeal. Consider again the courthouse at issue in *Cohen*. Why not allow unfettered speech in the courthouse? Surely it is implausible to think that citizens will stop showing up for city business, or will wear blinders and earplugs as they walk through the public halls. Just the same, it is implausible to think that the government will in response build fewer courthouses in an attempt to indirectly accomplish its original speech-restricting purpose. Thus, harnessing the captive audience in this instance would not lead to any significant behavioral responses. Society would end up with a new mechanism by which to promote exposure to diverse views, and that mechanism would come at relatively low cost given that neither unhappy citizens nor an unhappy government would do much to resist the effort. In short, captive audiences offer an inexpensive way to accomplish goals that society today accomplishes through the more costly mechanisms I outline above. That is not to suggest that every captive audience should be harnessed in this manner, or that using captive audiences in this way would fully obviate the need for those other approaches. My point is only that the existence of a captive audience should not be understood solely as a reason to regulate speech. Captive audiences can be put to beneficial use; that fact is ignored today in First Amendment jurisprudence.

Let me be more concrete. I propose here that the existence of a captive audience is properly understood as a reason to allow unfettered speech, and thus the burden on the government to justify a restriction on speech should be higher in instances where a captive audience is in play than it would be were there no captive audience present. With respect to public transportation systems, then, audience captivity should make us skeptical of a rule that bans advertisements. Why, we should ask, is the government wasting such a golden opportunity to promote diverse communication? In the courthouse, I would similarly be suspicious of any speech-restrictive rule. There might be good reasons for some such rules—perhaps a restriction is necessary to protect children from inappropriate images, or to ensure that court business can be conducted without too much distraction—but, whatever the reasons, I would judge them by a higher standard than that normally applied, precisely because a captive audience is too valuable an asset to without justification waste. Again, this is in contrast to current thinking, where the absence of audience self-help mechanisms is considered to be a reason to allow government regulation, not an argument against it.

This might sound crazy to some readers; but note that society in other settings already makes strategic use of captive audiences. For example, every four years the major television networks all simultaneously air the presidential debates. This is wasteful, in that the broadcasts are largely

redundant; but there is little public opposition because everyone understands that this is an attempt to create artificial captivity. If NBC were to offer the option of watching baseball instead of the presidential candidates, a good many citizens would accept the invitation.[25] Thus the Federal Communications Commission pressures NBC not to let viewers off the hook so easily, and the networks thereby together create a captive audience and use that audience to pass along hopefully revealing information relevant to the election.

My argument here is made in similar spirit. A captive audience is attractive because it offers an opportunity to pressure individuals to do that which they privately disfavor, and to exert that pressure at low cost in terms of unwanted self-help responses. The strategy should not be used to excess. But, where a captive audience naturally exists, the First Amendment should at least ask questions before allowing the government to waste the resource.

II. TRADE SECRETS AND THE ARMS RACE

I focused in the first part of this Essay on issues related to free speech, using the First Amendment to think through what are the two most intuitive statements about the relationship between legal rules and self-help remedies: namely, that the existence of cost-effective self-help remedies often argues against government regulation as a means to accomplish similar ends; and, conversely, that the absence of cost-effective self-help remedies often argues in favor. I turn now to trade secret law, and use those legal rules to consider another type of interaction: legal rules that cast self-help as a prerequisite to more formal interventions involving courts and government officials.

Start with some trade secret basics. Although the details vary state by state, trade secret protection is typically extended whenever three conditions are met. First, the information in dispute falls within the subject matter of the law, which under the Uniform Trade Secrets Act means that the information is not generally known and derives some economic value from its secrecy.[26] A customer list is a familiar example. Second, the qualifying information is taken by improper means, which is to say that a rival acquires the secret by engaging in trespass, inducing breach of contract, threatening violence, or otherwise either invading a protected legal interest or taking some action deemed to fall below acceptable standards of com-

---

[25] This happened in 2000, when NBC offered its affiliates the option of airing a baseball game rather than the first Bush/Gore debate, and FOX chose to premiere the science fiction thriller, *Dark Angel*. Both broadcasters were heavily criticized for their decisions. *See* William E. Kennard, *Fox and NBC Renege on a Debt*, N.Y. TIMES, Oct. 3, 2000, at A27 (Kennard was at the time Chairman of the Federal Communications Commission).

[26] *See* UNIF. TRADE SECRETS ACT § 1(4) (1985) (defining the term "trade secret").

mercial morality.[27] An example in the latter category might be dumpster diving, an act that is in many jurisdictions sufficient to support an allegation under trade secret law, but is not typically in and of itself a tort or trespass.[28] Third and finally, at the time of the improper taking, the information in dispute is the subject of reasonable precautions to maintain its secrecy.[29] This is a context-sensitive determination that might in one case require the use of a vault to store sensitive papers, while in another requiring that a particular facility be guarded around the clock.[30]

This last requirement is the specific requirement to which I alluded above: it denies a remedy to any trade secret holder who has failed to exercise reasonable self-help precautions. This is somewhat unusual. Property owners are not required to erect a fence in order to later sue an unwelcome visitor for trespass.[31] Automobile owners similarly need not prove that they locked their doors or used THE CLUB®[32] in order to qualify for police assistance in retrieving their stolen cars. Nor must creditors attempt self-help repossession prior to asking a court to transfer property that once served as collateral for a now-defunct loan.[33] Yet, to qualify for trade secret protection, trade secret holders must prove that their secrets were unveiled despite reasonable efforts to ensure its secrecy. Why?

One justification is that self-help serves to distinguish the bulk of normal business information from that special subset of information that war-

---

27 *See id.* at § 1(1) (defining the term "improper means").

28 See California v. Greenwood, 486 U.S. 35, 39 (1988) (holding in the Fourth Amendment context that there is no reasonable expectation of privacy in garbage left for disposal). *See generally* Harry Wingo, *Dumpster Diving and the Ethical Blindspot of Trade Secret Law*, 16 YALE L. & POL'Y REV. 195 (1997).

29 See UNIF. TRADE SECRETS ACT § 1(4)(ii) (defining the term "trade secret").

30 *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991) (discussing the precautions appropriate in a dispute involving product drawings). For an excellent introduction to trade secret law and its puzzles, *See* ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 27-104 (3d ed. 2003). A helpful introduction to the economics of trade secrecy can be found in WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 166-209 (2003).

31 In certain instances, hunters are allowed to trespass on private party unless the property owner has posted a sign notifying hunters that entry is not permitted. The practice is referred to as "posting the land," and the details vary considerably from state to state. *See* Tom Simmons, *Highways, Hunters, and Section Lines: Tensions Between Public Access and Private Rights*, 2 GREAT PLANTS NAT. RESOURCES J. 240, 250-54 (1997).

32 THE CLUB® is a commercial product that locks onto an automobile steering wheel and makes it difficult to drive the car. An owner who uses THE CLUB® thus reduces the likelihood that his car will be stolen, in that the thief now must not only hotwire the car ignition, but also somehow disengage THE CLUB®.

33 Creditors in certain instances have the option to engage in self-help repossession. But a creditor not interested in exercising this self-help option—say, for fear of legal liability if for some reason it turns out that the debtor was not in default—can, without any negative repercussions, choose to rely exclusively on judicial process. *See* U.C.C. § 9-503 (2004).

rants protection.[34] The idea is to keep the scope of trade secret protection in check by only protecting information in cases where the relevant trade secret holder signaled, up front, that the information was valuable. This is a task that seems unnecessary in the other examples. It is likely efficient to protect every piece of property from basic instances of trespass, to protect every car from unlawful access and use, and to allow every creditor to make good on the threat of taking possession of collateral in the event of a default. But it would be counterproductive to protect every shred of information from unauthorized dissemination, given that a modest flow of information across competitors surely stimulates innovation; and too restrictive a trade secret regime would impose huge administrative costs as parties would constantly fight over who learned what from whom. Thus the need to narrow and clearly mark that which is eligible for protection is a somewhat distinctive characteristic of trade secret law as compared to these other examples.[35]

A second justification is that self-help here provides circumstantial evidence that a given trade secret was taken unlawfully. A firm that mixes its secret chemical concoctions in a glass building would be hard pressed to prove that a rival took its secret by improper means. By taking precautions, a firm thus helps to establish at least a suggestion that there was an underlying bad act. There is less need for this type of evidence, by contrast, in my other examples, in that there will typically be reliable, physical evidence of a trespass; similarly reliable, physical evidence of automobile theft; and a clear document trail to establish the existence of a loan, the failure to pay that obligation, and the agreed-upon ramifications of that failure.[36] Just to be clear on what this means: I do not at all mean to imply that circumstantial evidence should suffice to prove a trade secret claim; there is always the very real possibility that the secret was taken by lawful means, and also the possibility that the secret was not taken at all but instead was independently discovered by the accused party. My point is only that, by requiring pre-

---

[34] *See* MERGES ET AL., *supra* note 30, at 50 ("one might treat the requirement of reasonable precautions as serving a gate-keeper function to weed out frivolous trade secret claims by requiring evidence of investment by the plaintiff in protecting the secret"); Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEGAL STUD. 683 (1980) (precautions serve to distinguish secrets from everyday unprotected information).

[35] Trade secret law could narrow and mark information in other ways. A neon sign would do the trick, as would a paperwork system where trade secrets holders record their interests in much the same way that security interests are recorded today. The key consideration is to ensure that in each case the relevant signal is sufficiently clear so as to keep administrative costs down, and sufficiently expensive such that trade secret holders face some pressure to choose a subset of information rather than protecting everything they know. Beyond that, plausible arguments can be made for a variety of signaling mechanisms, of which self-help in the form of reasonable precautions is just one.

[36] Some evidentiary disputes naturally remain in these other examples. My claim here is only that the lack of evidence would be an overwhelming problem in trade secret litigation but for the requirement that trade secret holders undertake reasonable precautions.

cautions, trade secret law removes from contention a category of cases where circumstantial evidence would not be available as a starting point for the analysis. The law might reasonably conclude that the costs of legal intervention in these precarious cases exceed any expected benefits.[37]

A third and final justification for trade secret law's reasonable precaution requirement is that such a requirement encourages firms to engage in self-help where that is the most efficient means by which to protect secret information. The idea here is that the law must sometimes encourage self-help, as the private incentive to engage in self-help does not necessarily well reflect the social payoffs. This is certainly true in other areas of the law. In tort law, for example, there is some question over whether accident victims would, if left to their own devices, take adequate precautions; and thus in many states rules of comparative and contributory negligence operate to reduce or eliminate damage awards in instances where the victim is himself at least partly to blame.[38] The common law similarly in many instances requires that an injured party mitigate his damages, again the requirement being justified on the ground that an injured party might not on his own mitigate even where that would be efficient.[39] In the context of trade secret protection, however, I must admit that I find this explanation rather weak. The problem is that, in most instances, private parties would choose to engage in reasonable precautions even if the law did not so require. No sense in hiring a lawyer when a simple fence will do! Given that, it seems relatively unconvincing to say that trade secret law requires reasonable precautions as a way of encouraging parties to take them.[40]

---

[37] For a parallel argument applied to copyright law—again the core insight being that many legal doctrines can and should exclude from protection cases that are prone to evidentiary complexity—see Douglas Lichtman, *Copyright as a Rule of Evidence*, 52 DUKE L.J. 683 (2003).

[38] My statement here obviously simplifies what has been a long-running debate in the economics literature over how best to encourage parties to take efficient precautions. For example, economic analysis under certain assumptions suggests that ordinary negligence rules already encourage efficient victim precaution, the reason being that a victim does not recover damages if the defendant took care but an accident occurred anyway. Under other assumptions—say, imperfect information—the analysis is less conclusive, and naturally there remain significant concerns in the context of strict liability. The details here are not central to my claims in the text; for citations and a nice overview, however, see Christopher J. Robinette & Paul G. Sherland, *Contributory or Comparative: Which is the Optimal Negligence Rule?*, 24 N. ILL. U. L. REV. 41, 51-53 (2003).

[39] For a helpful discussion of the mitigation doctrine and its applications within tort law and beyond, see Eugene Kontorovich, *The Mitigation of Emotional Distress Damages*, 68 U. CHI. L. REV. 491, 496-499 (2001). *See also* RESTATEMENT (SECOND) OF CONTRACTS § 350(1) ("damages are not recoverable for loss that the injured party could have avoided without undue risk, burden or humiliation").

[40] In other work, I have raised a similar argument regarding copyright law's requirement that, to be eligible for protection, a work must be fixed in a tangible medium of expression. Fixation has obvious virtues in that it increases the likelihood that the relevant expression will be passed from person to person, place to place, and generation to generation. Unfixed expression—say, an oral history or folktale—is more difficult to transfer and thus more likely to be lost. But, as I explain, that is not an argu-

More generally, most legal rules do not require self-help as a precondition to formal legal process, and I suspect that the reason is that the private incentive to engage in self-help is in most cases already sufficiently strong. Property law, for example, could require that every landowner put up a fence as a first barrier to unauthorized trespass; but why bother? Even without any legal obligation, most land owners install fences as needed. Why add another variable to trespass litigation by requiring landowners to prove the existence of a fence prior to alleging a trespass? Moreover, in those rare cases where a landowner fails to install a fence, it might be better to leave open the possibility of legal process rather than risking violence by denying the landowner any other remedy. This same logic also explains why the law does not require automobile owners to prove that they used car locks and other anti-theft devices. What a mess it would be to prove those facts in litigation, and there would be so little corresponding benefit given that most drivers lock their doors in any event. Creditors, too, will in most instances opt for self-help where that is truly the more efficient alternative, and thus a creditor's decision not to engage in self-help is again a judgment to which courts should likely defer.

None of this is to deny that there are instances where private parties do not have adequate incentives to engage in efficient self-help, and—as my tort and mitigation examples suggest—in those instances the law should and typically does cast self-help as a prerequisite to legal relief. But these are exceptions to the more common rule: where a party chooses not to attempt self-help, there are typically good reasons, as the private incentive to engage in self-help is naturally present and in most cases quite strong.[41]

The above all combines to explain why trade secret law casts self-help as a prerequisite to more formal legal protections; but consider now the inverse question of why, given the possibility of self-help, formal legal protections are available at all. Perhaps the most obvious answer is that in

---

ment in favor of the fixation requirement. After all, it is unlikely that requiring fixation actually increases the number of works that are fixed, because fixation is already cheap, easy, and significantly in an author's own interest. Thus, as it is with reasonable precautions in the trade secret context, the fact that society might want parties to engage in fixation is not itself a reason to require that act. See Lichtman, *supra* note 37, at 723-724.

[41] I focus in the text on cases where the private incentive to engage in self-help might be too low. Obviously, there are other settings where the private incentive might be too high. Drivers, for example, likely have too strong an incentive to protect their automobiles using THE CLUB®. The private benefits of this self-help precaution are high—THE CLUB® reduces the likelihood that the protected car will be stolen—but the social benefits are modest, given that THE CLUB® mainly encourages car thieves to substitute one theft for another. The proper legal response might be either to discourage use of THE CLUB®, or to subsidize alternative protections that actually reduce the incidence of car theft overall. LOJACK® might be one such alternative. *See* Ian Ayres & Steven D. Levitt, *Measuring Positive Externalities From Unobservable Victim Precaution: An Empirical Analysis Of Lojack*, 113 Q. J. ECON. 43 (1988) (arguing that LOJACK® does not have the substitution problem, primarily because LOJACK® is virtually invisible, and thus car thieves cannot determine which cars are protected and which are not).

many settings self-help precautions will fall short, failing to protect information that on policy grounds should be protected.[42] That is, it might be difficult to adequately secure a business facility from corporate espionage, and yet a limited ability to maintain secrecy is surely attractive, for the simple reason that secrecy encourages firms to invest in the development of new and useful information. Trade secret law thus fills an important void, creating that incentive and thereby acting as both a complement to and competitor for patent law.[43]

There is another and more striking answer to the question of why formal legal protections are layered on top of self-help remedies in this setting, however: trade secret law might simply serve to displace particularly wasteful forms of self-help. For instance, in the absence of robust legal protections, a concerned employer might inefficiently subdivide important tasks across employees in order to minimize how much any single employee knows about the firm. An employer might similarly put family members into sensitive positions rather than more qualified job applicants, the assumption being that family members are more apt to be loyal. The employer might even adopt strategies designed to restrict employee mobility (long-term stock options, for example, that vest only after a certain number of years of service) again as a mechanism by which to indirectly maintain control over firm secrets.[44] These are costly, second-best approaches;[45] if they cannot be easily regulated—and note how hard it would be to deter-

---

[42] Courts and commentators frequently invoke this explanation, emphasizing that trade secret law beneficially encourages innovation. *See, e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974); David D. Friedman et al., *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61 (1991). *But see* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 262-72 (1998) (questioning this justification on the ground that other legal regimes already promote innovation and protect valuable information sufficiently).

[43] Trade secret law on this theory should coordinate with patent law, pushing inventors toward the patent system in cases where eligibility and scope differences suggest that patent law might be the more attractive option from a social perspective, and attracting inventors where those same differences counsel the opposite result. To some degree, the law is consistent with this expectation, although the patchwork nature of the various legal doctrines does little to inspire confidence. For an overview, *see* ROBERT PATRICK MERGES & JOHN FITZGERALD DUFFY, PATENT LAW AND POLICY: CASES AND MATERIALS 565-68, 602-08, 611-13 (3d ed. 2002) (considering how the use of information as a trade secret reduces the possibility that the information can later be subject to patent protection).

[44] Many commentators believe that employee mobility facilitates innovation. *See, e.g.*, Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. Rev. 575 (1999); ANNALEE SAXENIAN, REGIONAL ADVANTAGE: CULTURE AND COMPETITION IN SILICON VALLEY AND ROUTE 128 (199). Employee mobility also has real value to employees, who might want to change employment for any number of valid reasons.

[45] *See* Bone, *supra* note 42, at 272-9 (summarizing various strategies like these, but then questioning whether legal process is in fact less costly than these wasteful alternatives), LANDES & POSNER, *supra* note 30, at 354-71 (identifying comparable strategies, and emphasizing that legal rules can in fact offer less wasteful mechanisms for achieving comparable ends).

mine whether information in a given firm was being inefficiently subdivided across employees, or whether family members were being favored because of their loyalty alone—the best response might be to acknowledge the problem and offer legal process as a substitute for these effective but wasteful methods.

Avoiding the costs associated with self-help is actually a common justification for legal rules that might on the merits be hard to explain. Patent law certainly benefits from this kind of second-best story, a story where trade secret protection itself plays the role of costly foil.[46] So, too, privacy protections. At first blush, modern law seems overly protective of personal privacy, restricting the disclosure of private facts related to personal finances, sexual orientation, medical conditions, and the like, even in instances where public revelation might serve social interests. Imagine, for example, if information about sexual promiscuity and sexual orientation could be acquired and disseminated without fear of legal liability. The former would do much to protect unsuspecting partners from the dangers of STDs, while the latter might significantly de-stigmatize what are still today controversial closet preferences.[47] Yet the law protects these facts.[48] and it arguably does so because, in the absence of protective legal rules, individuals would protect their privacy anyway, and would do so in ways that are more wasteful still. Patients would withhold vital information about their sexual history from doctors; adults discussing personal matters over the telephone would speak in tongues; and lovers interrupted in the privacy of their homes would on occasion resort to violence. Merits aside, then, privacy law might be explained simply on this notion that the law obviates the need for costly self-help measures.[49]

---

[46] *See* LANDES & POSNER, *supra* note 30, at 354 ("[T]he best economic justification for patent law is that it . . . curbs certain inefficiencies unavoidably created by trade secret law.").

[47] *But see* Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1041-3 (2003) (arguing that it is difficult to remove stigmas, often because there is a grain of truth hidden in otherwise distasteful judgments).

[48] This is accomplished not only through tort doctrines like those which prohibit unreasonable intrusion upon the seclusion of another—think here of wiretapping a phone, using binoculars to peer through a neighbor's window, or physically entering private premises uninvited—but also through related prohibitions on the unauthorized publication of already-discovered private facts.

[49] I should point out that privacy law does permit disclosure in instances where the revelation of a private fact seems to serve an immediate and important social interest. A psychiatrist, for example, can and indeed must break the doctor/patient privilege if he learns that his patient is about to commit a violent crime. *See* Tarasoff v. Regents of the University of California, 551 P.2d 334 (Cal. 1976). Medical professionals have similarly been held liable for failing to warn a patient's spouse that the patient was suffering from a dangerous and communicable disease. *See* Bradshaw v. Daniel, 854 S.W.2d 865 (Tenn. 1993). Recognizing exceptions, however, is a far cry from refusing to protect the information outright. With respect to STDs, for instance, it is implausible to think that a knowledgeable party will be able to identify in advance every vulnerable sexual partner and quietly warn that partner of the medical risks ahead. The exception in favor of such disclosures thus accomplishes little. The partner would be

On this general theme of how legal rules can be used to lure parties away from more costly forms of self-help, one special category merits particular attention: the arms race. In *E.I. du Pont deNemours & Co. v. Christopher*,[50] the chemical firm DuPont was in the process of building a plant at which the firm intended to use its secret but unpatented process for producing methanol. Access to the construction site was protected by fences and security personnel, the idea being to stop competitors from venturing onto the property and discovering the secret process by inspection. So a cunning competitor chartered an airplane to take pictures of the plant from above. DuPont filed suit, and the question before the court was whether this sort of aerial espionage was prohibited under Texas state law. The court noted that DuPont could have protected itself by covering the construction zone with a tarp, but nevertheless sustained the trade secret claim. Explained the court, "To require DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy's trick."[51] Thus trade secret law was used to avoid an arms race, with DuPont investing in guards and a fence, competitors procuring airplanes and cameras, DuPont responding with a tarp and perhaps radar detection, competitors returning with (say) satellite images and heat-sensitive camera technology, and so on and so on.[52]

Arms races like this one are remarkably common, and legal rules are often asked to reign in the resulting waste. That, however, is often an Herculean task. For instance, in response to online copyright infringement, copyright holders have in recent years worked feverishly to develop new technologies by which to protect their work from unauthorized duplication. As each new technology is unveiled, however, the hacker community responds, developing corresponding technologies for breaking encryption and freeing protected content.[53] The Digital Millennium Copyright Act was designed to slow this race—that Act makes it illegal to "circumvent a technological measure that effectively controls access" to a copyrighted work[54]—but the results have been disappointing, as hackers are difficult to identify,

---

much more richly protected in a world where information about sexual promiscuity were freely available. Privacy law does not take that step, however, because self-help makes that outcome unattainable.

50 431 F. 2d 1012 (5th Cir. 1970).

51 *Id.* at 1016.

52 Interestingly, one wonders why DuPont did not take the simple step of introducing some fake pipes into its plant design. That would have confused any aerial spies, and it would have cost much less money than either a tarp or litigation.

53 *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2nd Cir. 2001) (litigation over distribution of software that would allow for the unauthorized decryption of protected DVD content), Benny Evangelista, *Recent Cases Show Entertainment Industry's Difficulties in Locking Out Hackers*, SAN FRANCISCO CHRONICLE, May 3, 2001, at F1 (reporting on this and comparable disputes).

54 17 U.S.C. § 1201(a)(1)(A). *See also id.* §§ 1201(a)(2) & (b)(1) (further prohibiting firms from manufacturing or otherwise trafficking in technologies primarily designed to facilitate circumvention).

they often operate in foreign jurisdictions, and they rarely have the resources sufficient to pay legal judgments in any event.

Arms races can be difficult to stop for another reason: often the very acts that further a race are hard to distinguish from legitimate acts that courts are reluctant to prohibit. For instance, back when Internet search engines ranked results based on the frequency with which the chosen search term appeared on a given page, clever website owners would imbed valuable marks, and marks associated with their competitors, in unprinted parts of their websites and then repeat those terms so many times that search engines of the day would mistakenly think that these disingenuous websites were a good match for the search terms in question. Litigation against this practice moved forward under the trademark theory of initial interest confusion, a theory that basically forbids the use of a trademark to attract customer attention under false pretenses. But the law could never completely solve the problem. The reason was that many website operators had colorable good faith explanations. A former Playboy centerfold, for example, could justify using the Playboy mark, even if most of the viewers brought to her site were actually looking for the official Playboy page.[55] It was therefore difficult for trademark law to forbid the bad act that was driving the arms race without also interfering with perfectly legitimate trademark usage.

A similar problem has slowed efforts to thwart yet another Internet arms race, this one involving the various services that help end-users share music online. When the centralized Napster service was effectively shut down through legal action, it was replaced by decentralized alternatives like Grokster and KaZaA, services that are more difficult to stop because they have no central node through which all requests for music must pass. That change led to an arms race, with copyright holders using mislabeled decoy files to pollute the new networks,[56] while network designers worked to build reputation information into their architecture such that a user tricked by a decoy file could warn other users not to download that false file or even interact with the trickster who introduced it. As I say, the courts have had trouble slowing this particular race, the problem being that Grokster and KaZaA have legitimate uses. As with the Playboy example, that has made the courts reluctant to intervene, the fear being that any remedy effective

---

55 *See* Playboy Enterprises v. Welles, 279 F.3d 796, 804 (9th Cir. 2002) (former playmate allowed to use Playboy vocabulary because vocabulary did accurately identify her as a former playmate).

56 This sort of deception is a well-known mechanism by which to combat peer-to-peer file sharing. It frustrates users by tricking them into downloading the wrong songs, in that way making illegal music less convenient and hence marginally less attractive. Variants on the theme include uploading unpopular songs but labeling them as popular ones, uploading versions of the desired songs but garbling key sounds, and (my favorite) uploading versions of the desired song but interrupting the music with a message from the relevant artist chastising the supposed fan for acquiring music illegally. The term "spoofing" is used to describe a comparable practice. For discussion, see Doug Lichtman & David Jacobson, *Anonymity a Double-Edged Sword for Pirates Online*, CHI. TRIB., Apr. 13, 2000, at 25.

against illegitimate uses might inadvertently interfere with legitimate ones as well.[57]

Lest these examples be read to suggest that modern arms races are exclusively high-tech, consider the recent dispute between Major League Baseball's Chicago Cubs and the several firms that own rooftop properties overlooking the Cubs' home stadium, Wrigley Field.[58] At issue in the dispute were what are in essence unauthorized stadium skyboxes—complete with plush seats, fancy catering, and full service bars—built on these nearby rooftops and to which tickets are sold to watch Cubs baseball. The Cubs understandably thought these seats illegal; rooftop seats compete with stadium seats and yet the rooftop owners were contributing nothing toward team salaries or stadium upkeep. But copyright law offered no remedy. Courts are split over whether baseball games are eligible for copyright protection in the first place;[59] and, even if baseball games are eligible, the act of watching a copyrighted work without permission does not itself violate any of copyright law's exclusive rights.[60] While preparing to litigate state law claims sounding in misappropriation and unjust enrichment, the Cubs therefore triggered a little arms race: the team installed a large canvas windscreen that just so happened to block the view from several rooftop properties. The rooftop owners in response made plans to raise their rooftop seats higher; and, by the time a court began hearing the merits of the dispute, rumor had it that the Cubs were planning to construct a giant balloon that would have randomly obscured even elevated rooftop views. The arms race was abandoned when the parties came to terms last August. The rooftop

---

57 I say much more on this subject *infra* notes 99-113 and accompanying text.

58 *See* Jodi Wilgoren, *Cubs Sue Neighborhood Bars on Rooftop Use*, N. Y. TIMES, Dec. 18, 2002, at D4. I was directly involved in this particular dispute—I advised the Cubs on questions related to copyright preemption—so I should make expressly clear that the brief discussion here represents my own views, draws only on information publicly available, and should in no way be attributed to the Cubs, the team lawyers, or the team owners.

59 *Compare* National Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 846 (2d Cir. 1997) (games are not eligible for protection because they are competitive and have no underlying script) *with* Baltimore Orioles, Inc. v. Major League Baseball Players Ass'n, 805 F.2d 663, 669 (7th Cir. 1986) (player performances exhibit the modicum of creativity required for copyright eligibility). Interestingly, Dick Posner suggests that it might be sensible to allow baseball games to be protected because, in the absence of protection, an arms race would ensue, with game sponsors endeavoring to use contract law to restrict unauthorized access, and unauthorized viewers endeavoring to sneak a view by putting cameras in blimps or satellites. *See* Richard A. Posner, *Misappropriation: A Dirge*, 40 HOUS. L. REV. 621, 632-33 (2003).

60 See 17 U.S.C. § 106 (2004) (articulating the exclusive rights enjoyed by a copyright holder). The reason that there is no exclusive right related to unauthorized viewership is likely that such a right is in all but the most unusual cases unnecessary. Concert performers, basketball teams, and orchestras do not need this sort of legal protection to exclude uninvited guests; they already have effective self-help options in the form of gates, tickets, turnstiles, and guards.

owners agreed to share profits with the Cubs, and the Cubs in exchange agreed to engage in joint marketing with the rooftop owners.[61]

Legal rules that endeavor to stop arms races ultimately must confront three complexities, each implicit in the previous examples. First, there is the practical concern that efforts to stop an arms race will in fact merely redirect its energies elsewhere. After losing its trade secret case, do we really believe that DuPont's rival acquiesced, rather than instead looking to rent a faster airplane or an airplane that flies at higher altitudes, two among dozens of adjustments that would have made it more difficult for DuPont to detect the espionage in the first place?[62] Similarly, even if the courts had been quick to intervene in the Cubs dispute, how much would have been gained, given that the parties would have just shifted their dispute to the political arena, competing there in efforts to lobby local officials and sway public opinion?[63] This is not to imply that there is no value in shifting a race from one technology or venue to another; quite the opposite, each interaction imposes unique externalities, and each is subject to unique economic, technological, and political constraints. My argument is only that it is rare for law to completely disarm parties with adverse interests, and thus arguments predicated on the waste associated with self-help must always be sensitive to the realities of substitution.[64]

---

[61] *See* Jeremy Mullman, *Rooftop Rapprochement*, CRAIN'S CHI. BUS., Aug. 16, 2004, at A5. Experience with arms races like this one suggests that parties either do not accurately anticipate their rivals' responses, or that they do anticipate those responses but find it difficult to negotiate out of the interaction nonetheless. That is, one might imagine that the rooftop owners would have anticipated that the Cubs would install windscreens, and the Cubs would have anticipated that the rooftop owners would in response raise their seating, and so on; and that, armed with that knowledge, the parties would have been able to strike a bargain that would have avoided the costs of each side actually making good on its self-help threats. Yet, there was no such armistice. One reason might be that it is more difficult than it seems to predict the next move in the game, especially in a world where political pressure and public opinion might constrain particular parties at particular times. Another reason might be that there advantages to one or both sides from engaging in the race; for instance, the waste associated with the race might usefully pressure an otherwise reluctant court to intervene. *Cf.* Bone, *supra* note 42, at 275 (suggesting that a party will anticipate its rival's response and avoid waste accordingly, but then presenting a model to show that anticipation likely does not much reduce the overall expenditures made in the course of a race).

[62] Bob Bone also worries about this possibility. *See* Bone, *supra* note 42, at 276-279.

[63] Then again, there is reason to believe that the dispute here actually started in the political realm and only shifted to a physical and legal dispute after the political interactions were exhausted. *See* Wilgoren, *supra* note 58 (noting two years of talks that preceded the litigation and involved the various parties as well as Chicago city officials).

[64] Government efforts to thwart races are often limited by the reality of substitution. The "prospect theory" of patent law, for example, suggests awarding an early, broad patent that covers a large field of endeavor in order to reduce the waste that would be incurred were multiple inventors free to compete to develop the many inventions covered by the broad patent. *See* Edmund Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265 (1977). A problem with the theory is substitution: patent protection accelerates the race to an earlier stage, with inventors now racing to claim the broad, early patent. *See* Donald G. McFetridge & Douglas A. Smith, *Patents, Prospects, and Economic Surplus: A*

Second, arms races are not always harmful, and the law must therefore be careful to identify those rare but important races that ought to be allowed to continue. The Cubs dispute offers an example of a purely wasteful race: it is implausible to suggest that the introduction of windscreens enhanced the experience for fans in either location, and raising the height of rooftop seating at some point not only introduces serious safety concerns but also obscures the view of the field.[65] Contrast that, however, with the race that surrounds the distribution of copyrighted materials online. Now admittedly there is substantial harm inherent in that race: the introduction of decoy files, for example, exhausts bandwidth that could be better used for legitimate exchanges of information; and the entire interaction poses a real threat to the overall integrity of the copyright system. But, on the bright side, the back-and-forth over encryption and distribution technologies has inspired a great many young people to think about new protocols for Internet communication and new concepts in network design. They might be doing so for all the wrong reasons; but, thanks to the copyright wars, a creative and sophisticated intellectual resource—one that might have been impossible for society to in other ways tap—has contributed, perhaps substantially, to advances in Internet technologies. That last step is important. Almost every race has some plausible spillover benefit; what is unique about the copyright arms race is that the spillover benefit would have been all but impossible to achieve but for the race.

The arms race in the previous example is attractive because of the activities undertaken in the process of racing. Consider now an example that is attractive instead because of the outcomes the race makes possible. Under conventional trade secret principles, a competitor is permitted to purchase a rival's product, smash it to pieces on the ground, and then study those remnants to learn whatever secrets they might reveal.[66] This is re-

---

Comment, 23 J.L. & ECON. 197 (1980). Similarly, for many years, local communities had only one cable licensee and only one authorized local telephone provider, the worry being that having multiple providers would lead to wasteful duplication of the telephone and cable grids, respectively. *See* Omega Satellite Prods. Co. v. City of Indianapolis, 694 F. 2d 119, 126 (7th Cir. 1982) (Posner, J.). Substitution again gummed up the works: waste was incurred in a new form, as firms fought in the public and political arenas to increase their chances of being chosen the lucky winner. *See* Aditya Bamzai, *The Wasteful Duplication Thesis in Natural Monopoly Regulation*, 71 U. CHI. L. REV. 1525 (2004). The lesson in each of these examples is the same: it is difficult to stop private parties from racing, and thus the focus of the law should be to choose the race that has the most attractive cost/benefit profile. *Cf.* John Duffy, *Rethinking the Prospect Theory of Patents*, 71 U. CHI. L. REV. 439 (2004) (defending the prospect theory on the ground that an accelerated patent race has real allure: it forces earlier patenting, and in so doing moves the relevant patent's expiration date earlier in time).

65 Perhaps this is why the case ultimately settled. Both sides recognized that racing was expensive and was producing little value for Cubs fans.

66 Reverse engineering can take other forms, like testing the properties of a competitor's product or decompiling a competitor's computer code. *See* UNIF. TRADE SECRETS ACT § 1 cmt. 1 (amended 1985) (identifying as a proper means of discovery the act of taking a "known product and working backward to find the method by which it was developed").

ferred to as reverse engineering, and just like every other means by which one competitor might learn secrets from another, reverse engineering triggers self-help responses. For instance, because reverse engineering is permissible, firms have an incentive to introduce unnecessary complexity into their products in an effort to stymie reverse engineering attempts. Firms also have an incentive to distort the design of their products and services, perhaps favoring designs where the critical step is accomplished by a software process rather than (say) a more transparent hardware product. Reverse engineering, then, spawns a classic arms race; but trade secret law nevertheless allows it on the theory that the additional exchange of information made possible by reverse engineering more than compensates for the waste. Reverse engineering is an attractive means by which to accomplish this function because reverse engineering need not be done in the presence of the trade secret holder and thus it is unlikely to disrupt the trade secret holders' business operations or lead to physical confrontation.[67]

Third and finally, note that the mere existence of a wasteful arms race does not by itself offer any insight into which party ought to be favored in any resulting legal intervention. Recall once more the dispute involving DuPont. That DuPont and its rival were on the verge of an arms race is clear; but reasonable minds might disagree as to whether the best result would have been to stop the arms race and recognize a legal interest in favor of DuPont, or stop the arms race and recognize instead a legal interest that would allow rivals a glimpse at the disputed trade secret. An argument in favor of the former approach would emphasize the importance of allowing DuPont to earn a return on the investment it made in developing its secret process. An argument in favor of the latter approach would stress the benefits of allowing firms to learn from one another, cross-pollinating in much the same way championed by the privilege in favor of reverse engineering. Interestingly, the court had only one of these options at hand: it

---

[67] Although I believe that reverse engineering should often be permissible, I am skeptical of the privilege in certain applications. For example, some types of reverse engineering are so cheap that they threaten to fully undermine the incentive to engage in innovative activity in the first place. In those circumstances, it might be attractive to allow for some form of prohibition against the cheap copying technique. *See* Douglas Gary Lichtman, *The Economics of Innovation: Protecting Unpatentable Goods*, 81 MINN. L. REV. 693 (1997). Similarly, reverse engineering sometimes undermines a type of coordination that might otherwise benefit both an industry and its customers. Because of this, manufacturers of new computer platforms—a new handheld computer or a new video game system—might need some protection against reverse engineering, protection sufficient to allow the platform owner to coordinate the development of complementary goods like software and hardware peripherals. *See* Douglas Lichtman, *Property Rights in Emerging Platform Technologies*, 29 J. LEGAL STUD. 615 (2000) (explaining how coordination benefits both producers and consumers). Other academic authors have raised their own concerns about reverse engineering, although in the end most of us think that reverse engineering should typically be allowed. *See, e.g.*, Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575 (2002) (discussing situations where reverse engineering is and is not attractive); LANDES & POSNER, *supra* note 30, at 369-71 (same).

could sustain DuPont's claim of a violation of trade secret law and thereby assign the property right to DuPont. There was no plausible counterclaim—unlawful interference with an aerial view?—that would have empowered the court to assign the right in favor of the spying competitor. This is something of an aberration, however; in most instances, the court has before it legal claims sufficient to assign the relevant right to either litigant, and the puzzle comes only in deciding which party wins on the merits.

III. COPYRIGHT AND COPYRIGHT INFRINGEMENT

Thirty years ago, the only significant self-help mechanism available to an author who wanted to maintain control of his work was to keep the work confidential. Once a work went public, its author had no choice but to turn to copyright law for any semblance of control over reproduction, dissemination, adaptation, and performance. As a result, authors also had no choice but to accept the constraints that came along with federal rights, constraints like the fair use doctrine,[68] the first sale doctrine,[69] and limitations on the ownership of facts and ideas.[70] This landscape changed significantly, however, with the introduction of "digital rights management" and related mechanisms that allow content owners to opt out of copyright law and instead rely on encryption and monitoring technologies to control access to their work. Encryption and monitoring allow a content owner to package content such that it (say) stops functioning after a predetermined number of uses, or can be accessed only from a specifically licensed geographic location. The implication is not merely that authors can use technology to expand on copyright law's default package of rights while rejecting copyright law's policy-motivated limitations, but also that authors can use technology to assert control over phone books, databases, and other subject matter that the copyright system would leave in the public domain.

How much of a change this will turn out to be is admittedly a difficult question, but four factors suggest that the change might not be particularly severe. First, hackers have thus far been remarkably effective at defeating digital rights management systems, freeing protected content and rendering implausible the fear that every scrap of content will soon be trapped behind lock and key. Put differently, unauthorized duplication and distribution is a

---

[68] 17 U.S.C. § 107 (2004) (excusing infringement in certain cases based on an open-ended policy inquiry).

[69] 17 U.S.C. § 109(a) (2004) (authorizing the owner of a copy of a copyrighted work to resell or otherwise transfer his legitimate copy without the need for explicit permission from the copyright owner).

[70] 17 U.S.C. § 102(b) (2004) (excluding from protection ideas, facts, and related non-expressive elements); Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340 (1991) (discussing and arguably expanding this principle).

far more pressing problem than is digital rights management; that has been true over the last ten years, and seems likely to remain true for the foreseeable future. Second, consumers seem to disfavor protected content and other rights-limiting technologies, and thus there is significant financial pressure not to adopt digital rights management. Third, even at the theoretical extreme, digital rights management can only be so controlling. It is hard to imagine how any technology could stop a person from hearing a song and then later humming it in the shower or creating a humorous parody. Indeed, the Achilles' heel in every system designed to control access to content is that at some point customers must be able to read, hear, or otherwise experience the purchased information. Whenever that happens, the information is necessarily vulnerable. Fourth and finally, content producers do not necessarily want airtight control over their work in any event, and thus there is no reason to expect that content owners will use extreme forms of digital rights management even if extreme forms were to become available. Magazine publishers, for example, likely benefit from the fact that consumers share magazines, passing a given issue from one friend or family member to another. The reason is that sharing in this manner is a less expensive way to distribute magazines than is the next-best alternative: printing, packaging, and shipping another copy. Thus, as long as a publisher can increase the price of the original magazine issue to compensate for expected patterns of sharing, the publisher has little incentive to thwart the practice. Sharing makes everyone better off, with both publishers and consumers benefiting from the savings made possible through the use of a cheaper distribution channel.[71]

All this is not to dismiss the possibility that digital rights management might someday overstep proper bounds and at that moment warrant a response. The question would then become how best to discipline this form of self-help. One option would be to rely on consumers to develop their own counter-measures, answering new encryption technologies with new

---

[71] See Stanley M. Besen & Sheila N. Kirby, *Private Copying, Appropriability, and Optimal Copyright Royalties*, 32 J.L. & ECON. 255 (1989) (modeling this type of interaction). *See also* Yannis Bakos, Erik Brynjolfsson & Douglas Lichtman, *Shared Information Goods*, 42 J.L. & ECON. 117 (1999) (arguing that small-scale social sharing is attractive to content producers even in instances where the costs of duplication and distribution are trivial, specifically because small-scale sharing facilitates a subtle form of price discrimination). The literature on digital rights management typically blurs an important distinction relevant to this question of whether content owners want absolute control: the distinction between perfect price discrimination—where a seller knows exactly how much a given consumer values a given content product and can price accordingly—and control of the sort I discuss in the text, where a seller at best might know how often a consumer listens to a given song, and when, and from where. To be sure, the latter is a proxy for the former, but it is not a substitute. Knowing how often you listen to a given music CD might hint at how much you value it, but there is slippage between these two types of information. Content holders admittedly would love to be able to practice perfect price discrimination. But that does not imply that they also will use technology to exercise complete control. As the magazine example makes clear, control might not be in their interest, even though price discrimination clearly is.

decryption techniques, and offsetting increased content control with expanded efforts at unauthorized duplication and distribution. The drawbacks to this approach are many, in that the result is an arms race—recall the discussion on point in the previous section—and, besides, there is no reason to believe that this back and forth will yield anything close to an optimal division between rights and restrictions. Another option would be to regulate encryption technologies directly. The federal government has never explicitly regulated the use of encryption technologies domestically, but there have long been export restrictions in place,[72] and law enforcement authorities do from time to time urge that manufacturers be required to build backdoors into otherwise-secure telecommunications equipment so as to facilitate government access under appropriate conditions.[73] Regulation along these lines might be particularly effective in the copyright setting because the encryption at issue would be used in mass-market products. Regulations targeting criminal or other unlawful encryption, on the other hand, have always been hard to enforce because the relevant products and people are typically operating underground.

A third and more distinctive response to digital rights management might come through the doctrine of copyright misuse. Copyright misuse is an equitable defense to copyright infringement. It immunizes an infringer from liability in cases where the infringer can show that the relevant copyright holder has, in this or some unrelated interaction, used the relevant copyright "in a manner contrary to public policy."[74] An example of a copyright holder potentially vulnerable to the defense would be a software firm whose contracts forbid licensees from reverse engineering copyrighted computer code. A court might in response invoke the doctrine of copyright misuse and refuse to enforce the implicated software copyright in any dispute—even one completely unrelated to reverse engineering—until the disfavored practice is stopped and its ramifications on the market undone.[75]

---

[72] For detailed discussion, see Tricia E. Black, *Taking Account of the World As it Will Be: The Shifting Course of U.S. Encryption Policy*, 53 FED. COMM. L.J. 289 (2001).

[73] For discussion of one such proposal, see Christopher E. Torkelson, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 SETON HALL L. REV. 1142 (1995). Eric Posner and I have advanced our own variant on this idea, urging that Internet service providers be obligated to store information at the government's request even in situations where the government cannot at the time convince a court that the government should be allowed to also look at the stored information. In essence, our argument is that the standard for requiring storage of information should be lower than the standard for allowing inspection of that information, the reason being that the extra storage preserves for society the option to later authorize inspection as new information reveals that to be appropriate. *See* Douglas Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, SUP. CT. ECON. REV. at manuscript n.40 (forthcoming 2005).

[74] Lasercomb Am., Inc. v. Reynolds, 911 F.2d 970, 979 (4th Cir. 1990). As copyright misuse becomes a more influential doctrine, courts or Congress will need to sharpen its contours, as a vague inquiry into what is "contrary to public policy" seems dangerously ripe for error, uncertainty, and abuse.

[75] Marshall Leaffer considers the specific question of whether software owners should be subject to the misuse doctrine on these facts in Marshall Leaffer, *Engineering Competitive Policy and Copyright*

Like any unclean hands doctrine, the principal charm of copyright misuse is that it can be used to discipline behaviors that are difficult to regulate directly. No need to catch a copyright holder actually encrypting his work, or to wait for a specific dispute involving the encryption scheme per se. Instead, copyright misuse comes into play the moment the relevant copyright holder turns to the courts for help in enforcing any aspect of the implicated copyright. This is also the central limitation on the doctrine: it has no bite as applied to content producers whose self-help options are so appealing that they have no need for copyright.[76] Luckily, however, few copyright holders will fall into that category, given that copyright will maintain its importance with respect to certain classes of violations—say, unauthorized public performance—even if it loses its primacy with respect to others.[77] That is, there is no technology that will stop unauthorized bands from publicly performing songs from Madonna's latest album; thus, even in a world where Madonna can use encryption to protect her album from unauthorized distribution, she will still turn to copyright to stop other behaviors of which she disapproves.[78] Misuse could therefore effectively pressure Madonna and similarly situated copyright holders to choose between copyright law and self-help, taking away the option of using both regimes to protect any single copyright-eligible work.[79] The result would be less dra-

---

Misuse, 19 DAYTON L. REV. 1087 (1994). Other commentators have suggested that misuse be used to respond to other forms of overreaching by copyright holders. *See, e.g.*, Lydia Loren, Slaying the Leather-Winged Demons in the Night: Reforming Copyright Owner Contracting with Clickwrap Misuse (Working Paper 2004) (on file with author) (misuse should apply in instances where copyright holders assert impermissibly broad rights in contracts and other forms of licensing agreements); Dan Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095 (2003) (misuse should be used to punish copyright holders who abuse the anti-circumvention provisions of the Digital Millennium Copyright Act).

[76] The opposite problem also warrants attention: when a court uses copyright misuse to punish a copyright holder for its bad acts, there is no guarantee that the punishment will be remotely proportionate to the crime. Because misuse is an equitable doctrine, however, it is possible that courts can and will address this problem by limiting the instances where misuse can be invoked, or enforcing the copyright to some degree even in instances where misuse rightly precludes complete enforcement.

[77] This argument does not resonate where the economic value of the work in question can be fully protected by encryption and monitoring technologies. Databases might be one important example. Once encryption technology matures, database owners might not need any additional support from copyright or comparable laws, and thus the threat of misuse and related unclean hands doctrines might not much alter behavior. In such cases, either direct regulation will be necessary, or the unclean hands rules will have to expand to take away other causes of action that might still be valued by the relevant private parties, such as causes of action related to trade secrecy or the enforcement of contracts.

[78] For ease of exposition, I assume in the text that Madonna holds copyright not only to her sound recordings, but also to the underlying musical works. The analysis does not change if we assume more complicated ownership structures.

[79] An interesting question to ask is whether misuse should focus on a single work, or should instead treat together several copyrighted works owned by the same private party and perhaps related to one another as either complements or substitutes. The law as it stands applies to each copyrighted work in isolation, but that might not be the right design in a world where copyrighted works are often sold and

conian that an absolute prohibition on self-help because it would leave copyright holders with the option of using self-help instead of law;[80] and it also would be easier to enforce, given that courts implement the doctrine simply by declining to act when called upon to do so by a disfavored copyright holder.

My discussion thus far has focused on self-help technologies that allow copyright holders to assert greater control over their work. Turn now to the opposing self-help technologies through which college students and other ordinary consumers are themselves shifting legal boundaries, specifically by engaging in the unauthorized duplication and dissemination of copyrighted work online. Copyright law has had a hard time discouraging illegal activities of this sort, the primary reason being that the large number of bad actors makes normal legal process prohibitively expensive. The law could in theory still deter either by significantly increasing the penalties associated with these illegal acts, or by finding some strategy to lower the cost of bringing each individual case.[81] Neither approach, however, holds great promise.

With respect to increased penalties, current penalties for copyright infringement are already quite steep, with statutory damages clocking in at anywhere from $750 to $30,000 per work copied,[82] and criminal prosecution a real possibility thanks to renewed interest from the Department of Justice.[83] A college student with a modest collection of illegal music is therefore already being threatened with a possible punishment on the order of five years in jail[84] and well over $500,000 in cash damages. It is hard to imagine credibly threatening higher penalties for this category of legal wrong; and, even now, nearly every case settles for a tiny fraction of the maximum possible penalty, presumably because both the government and

---

used in bundles. Then again, a doctrine that lumped several copyrighted works together might unfairly penalize large firms, given that large firms typically own a large number of copyrights.

80 As I mentioned earlier—see text near note 75—misuse is less draconian in another way: it allows copyright holders to change their mind, abandon their self-help mechanisms, and return to the protections offered by copyright. The only limitation is that legal protection will not begin again until the effects of the earlier self-help have been fully dissipated. Whether this is a virtue or a defect obviously depends on how strongly society wants to bind copyright holders to their self-help choices.

81 This understanding of deterrence derives from Gary Becker's original insight that, in instances where the likelihood of detection is low, deterrence can be achieved by increasing the penalty imposed. *See* Gary Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968).

82 17 U.S.C. § 504(c). Downward and upward departures are available where infringement can be shown to be either innocent or willful, respectively. *See id.* at § 504(c)(2) (innocent infringement can be as little as $200 per work, while willful infringement can be as much as $150,000 per work).

83 *See* Saul Hansell, *U.S. Searches Computers, Trying to Disrupt Piracy*, N.Y. TIMES, Aug. 26, 2004 at C4 (describing the Justice Department's intensifying efforts to crack down on illegal file sharing).

84 Under the No Electronic Theft Act, there are different offense levels, and each carries its own range of possible sentences. *See* 18 U.S.C. § 2319 (establishing fines and permissible sentence ranges).

the copyright industry feel constrained by the possibility of negative publicity.[85]

Meanwhile, although the idea of lowering the costs of legal process resonates in the abstract, in practice none of the plans proposed thus far show much promise. For example, over a several month period in 2003, the Recording Industry Association of America experimented with a streamlined court process wherein copyright holders would present circumstantial evidence of online infringement to a court clerk and, in response, the clerk would issue a subpoena ordering the relevant Internet service provider to reveal the name and address of the accused infringer.[86] The process was designed to avoid the expense of conducting a full hearing before issuing each subpoena; in particular, it cut corners by relying on a court clerk rather than a judge, and by not offering accused parties the opportunity to defend their anonymity through counsel. The procedure, however, was roundly criticized for fear that it would be too easily abused. Worries included somewhat outlandish concerns that stalkers, pedophiles, and the like would masquerade as injured copyright holders in order to discover the names and addresses of previously anonymous targets; but they also included more plausible privacy and due process concerns over a streamlined process that unmasked anonymous parties without giving them any chance to anonymously resist.[87] The merits here were never adjudicated; the D.C. Circuit killed the program on the ground that it was not authorized by statute.[88]

---

[85] This has another cost: it likely reduces respect for the law. College students are learning the lesson that society will not stick to its guns when it comes to enforcing the law as written or collecting the penalties the law threatens. That might not be particularly important when it is only copyright law at stake, but I wonder if the lesson can be so easily cabined, or if instead the experience with copyright law over these last several years will in the future undermine respect for legal rules more generally.

[86] The music industry interpreted a provision of the Digital Millennium Copyright Act to authorize this fast-track procedure. *See* 17 U.S.C. § 512(h) ("A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.").

[87] *See* Amy Harmon, *In Court, Verizon Challenges Music Industry's Subpoenas,* N.Y. TIMES, Sept. 17, 2003 at C5. It is interesting that Verizon, an Internet service provider, was the most vocal champion of the privacy, due process, and statutory objections. A cynical explanation is that Verizon had ulterior motives given that consumer interest in online piracy likely drives demand for Internet access, and Verizon makes money selling additional phone lines, DSL connections, and Internet service more generally. And, while admittedly Verizon would also earn additional revenues were legal alternatives like iTunes to become more popular, there is no incentive for Verizon to choose. Verizon can promote both alternatives, and make money by selling Internet access to legitimate and illegitimate users alike.

[88] *See* RIAA v. Verizon Internet Servs., 351 F. 3d 1229 (D.C. Cir. 2003), *cert. denied* 160 L. Ed. 2d 222 (2004). My own opinion is that the fast-track approach was unnecessarily threadbare—too quick to force Internet service providers to name names, too willing to proceed without opportunities to double-check allegations and otherwise ensure good faith. A better approach would have been to require firms like Verizon to deliver warnings to accused subscribers, reminding subscribers that piracy is illegal and that "the copyright holder might take his evidence to court and, after a hearing where you will have the opportunity to defend yourself anonymously through counsel, the court might order us to

More recently, Professors Mark Lemley and Anthony Reese have proposed their own fast-track approach,[89] a dispute resolution system that would keep costs down by allowing a copyright holder to establish a prima facie case simply by: (a) submitting a sworn statement asserting that the complaining entity is in fact the relevant copyright holder;[90] (b) providing evidence that the copyrighted work at issue was available for downloading from a particular Internet address at a particular date and time;[91] and (c) providing evidence linking the implicated Internet address to a particular accused infringer.[92] If, after such a showing, the accused infringer fails to contest these facts, Lemley and Reese would allow their dispute resolution system to proceed to final judgment. If the infringer instead introduces "a plausible claim of mistaken identification" or other evidence that casts doubt on the prima facie case, however, Lemley and Reese would refer the case to the federal courts for a fuller hearing.[93]

The problem with this approach is that it is only trivially cheaper than normal litigation. That is, under the current system, if a copyright holder has evidence of a valid copyright, has evidence that the copyrighted work was made available online without permission, has evidence linking that bad act to a specific person, and faces an accused infringer who is not able or willing to contest any of those factual predicates—the four essential requirements in the Lemley/Reese arbitration—the costs of litigation are already quite small. In fact, such cases typically settle after the first legal document is filed,[94] and that first document is typically cheap to draft given that it is basically a form document that every time recounts the same legal argument, the same basic assertions of wrong-doing, and so on. Framed another way, the costs that make copyright enforcement expensive are the

---

reveal your identity and provide further evidence of your alleged bad acts." Imagine the shiver that would go down an infringer's spine upon finding that note in his inbox, complete with a specific accusation that the user had downloaded Madonna, last Tuesday, at midnight, from the bedroom computer. Were such warnings delivered quickly, a brief delay before revealing the infringer's name and address would be less costly, which is to say that copyright holders would on these facts not be significantly harmed by a process that took a little more time to confirm that the accused infringer really should be unmasked.

89 Mark Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345 (2004).

90 *Id.* at 1414.

91 *Id.* ("Such evidence could consist of, for example, screen shots showing the availability of files and a sworn statement that the copyright owner determined that the titles listed were actually available and were actually copies of the copyrighted works.").

92 *Id.* (noting that this evidence would typically need to be obtained from the user's service provider).

93 *Id.* at 1415, 1417 (a plausible claim of mistaken identification is sufficient to have the dispute dismissed without prejudice; certain defenses must be raised in the federal courts after the prima facie evidence is evaluated by an administrative law judge).

94 Most of the suits against individual infringers have thus far settled. *See, e.g.*, Jon Healey, *File Sharing Down After Lawsuits*, L.A. TIMES, Sept. 30, 2003 at C15 (reporting first 54 settlements).

ones to which the Lemley/Reese proposal does not speak: the costs of associating an Internet address with a specific flesh-and-blood person (Internet service providers have this information, but they rarely are willing to provide it absent a court order to do so[95]); the costs of rebutting plausible defenses related to fair use and mistaken identity; and the costs of enforcing judgments.[96] These costs are admittedly difficult to reduce. But, without such reductions, there is little hope for streamlining the litigation process.[97]

Where deterrence at the individual level cannot work, the typical response is to regulate or in other ways hold accountable parties that facilitate

---

[95] As I mentioned *supra* note 87, this might be self-serving behavior on the part of the Internet service providers. But it might also be an important dimension along which service providers compete. Consumers, and especially consumers with something to hide, might flock to the provider who most credibly promises not to reveal subscriber identities.

[96] Lemley and Reese suggest that the costs of enforcing judgments might not be steep. *See* Lemley & Reese, *supra* note 89, at 1420-1422. If they are right, my criticism still holds. After all, the various reasons they list for why enforcement might be cheap in the context of their arbitration process apply with equal force to the normal judicial process. My concern thus remains: I do not see how their approach more than trivially reduces the costs of litigating infringement cases.

[97] Two other concerns related to the Lemley/Reese proposal bear mention. First, as Lemley and Reese themselves point out, their procedure would work only for large-scale pirates. *See id.* at 1413 n.274. That is a severe limitation, given the obvious evolutionary response: the topography of infringement will change from the current pattern where a small number of users contribute the vast majority of songs, to a new pattern where every user offers up only a handful of songs. The Lemley/Reese arbitration would, by virtue of that adjustment, be fully de-toothed, and yet little would change in terms of aggregate illegal behavior. *Cf.* Lior Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505 (2003) (discussing ways in which peer-to-peer networks encourage small-scale sharers to increase their participation).

Second and perhaps more important, the Lemley/Reese approach rises or falls on their assertion that (to quote their title) it is possible to "reduc[e] digital copyright infringement without restricting innovation." That is, Lemley and Reese want copyright holders to be able to hold college students accountable for their illegal use of peer-to-peer technology, and they favor that approach because alternative approaches—like holding technology firms accountable—would reduce the incentive to create and disseminate similar technologies in the future. That sounds right at first blush, but the argument falters when one realizes that their system, too, reduces the incentive to create and disseminate these technologies, because the real spur to innovation here is copyright infringement. Phrased another way, if I am wrong in my criticisms thus far and the Lemley/Reese proposal does significantly deter copyright infringement by making available an arbitration system, the incentive to create and disseminate the next Napster will be ruined anyway. The average person will not pay a scrap of attention; the overwhelming reason why people download these sorts of new technologies and experiment with them is simply to get access to copyrighted songs. Without infringement driving demand, these technologies die on the vine. The Lemley/Reese argument thus strikes me as a bit unfair. Their Article criticizes other approaches on the ground that those approaches reduce the incentive to innovate, but the Article never concedes that the arbitration approach suffers a very similar flaw. Indeed, my own hunch is that an effective arbitration system would do more damage than would other approaches, in that the threat of arbitration would discourage college students from playing with these technologies, thus ruining the precise mechanism that brought us file-sharing software in the first place. The better approach is to hold responsible the firms that profit from infringement online, perhaps forcing them to pay modest damages or requiring that they design their systems in ways that better respect copyright rights. That would protect copyright to some degree, but still recognize in the college students a certain freedom to tinker.

the illegal practice.[98] Copyright holders have obviously attempted that strategy, perhaps most notably through high-profile litigation against Internet startups Napster,[99] Aimster,[100] and Grokster.[101] Much has already been written on these particular cases,[102] as well as on the general issues they raise,[103] and I will therefore keep my remarks on this topic short. I want to emphasize, however, that these are difficult cases because the technologies at issue are capable of both legitimate and illegitimate use. That is important as a matter of copyright doctrine—two decades ago, the Supreme Court found manufacturers of video cassette recorders immune from copyright liability primarily on the ground that VCRs are "capable of substantial noninfringing uses"[104]—and as a matter of policy as well, in that courts when faced with dual-use technologies must be careful not to regulate in a way that unnecessarily discards the wheat with the chaff. At the same time, caution should not be allowed to morph into paralysis, especially in instances where small modifications to the relevant technology could reduce the number of illegitimate acts without substantially interfering with legitimate ones, or substantially altering the core underlying technological accomplishment.[105]

---

98 For a general introduction to the economics of indirect liability, *see* Lichtman & Posner, *supra* note 73 (discussing the intuitions and limitations, and then applying those concepts to the question of whether Internet service providers should be held liable for their role in propagating viruses, worms, and other forms of Internet mischief).

99 *See* A&M Records v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

100 *See* In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

101 *See* MGM Studios, Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir.), *cert granted* 125 S. Ct. 686 (2004).

102 For one early and insightful discussion, see Stacey L. Dogan, *Is Napster a VCR? The Implications of Sony for Napster and Other Internet Technologies*, 52 HASTINGS L.J. 939 (2001).

103 *See, e.g.*, Randal C. Picker, *Copyright as Entry Policy: The Case of Digital Distribution*, 47 ANTITRUST BULL. 423 (2002); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003); Lemley & Reese, *supra* note 89; WILLIAM FISHER, PROMISES TO KEEP: TECHNOLOGY AND THE FUTURE OF ENTERTAINMENT (2004); Neil W. Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 2 (2003).

104 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

105 Applause on this score to the district court in the Northern District of California that ordered Napster to undertake narrow, specific efforts to exclude copyrighted music from Napster's master list of available downloads. For example, the court ordered Napster to block titles explicitly identified by copyright owners as ones being traded or likely to be traded on the network. And, recognizing that clever users would respond by introducing obvious typographical errors into song titles—one popular approach was to list each title in pig Latin—the court ordered Napster to "use reasonable measures in identifying variations of the filename(s), or of the spelling of the titles or artists' names, of the works identified by plaintiffs." A&M Records, Inc. v. Napster, Inc., 2001 U.S. Dist. LEXIS 2186, at *5 (2001). The *Grokster* court, by contrast, declined to issue an injunction of this sort, not even broaching the question of whether a peer-to-peer system could be modified in ways that would encourage respect for copyright law without sacrificing the distinct benefits of peer-to-peer architecture. *See* Grokster, *supra* note 101, at *29.

Let me unpack those concerns just slightly further.[106] In *Sony Corporation of America vs. Universal City Studios, Inc.*, the Supreme Court held that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses."[107] Bill Landes and I have criticized this holding along two dimensions. First, read literally, it fails to account for the costs and benefits of the technology at issue, excusing from liability even a product for which expected harms fully overwhelm expected benefits. There are admittedly reasons not to engage in too careful a cost/benefit balance. It might be difficult for a court to predict future uses of a new technology; and some harmful uses ought not count given that they can be better addressed through other forms of intervention, such as direct litigation against the relevant bad actors and self-help.[108] However, on its face, the *Sony* rule requires no balancing at all; and, if that reading is correct, it seems an unduly paranoid approach.[109]

Second, the *Sony* rule creates no incentive for firms to try to protect copyright. Instead, it offers blanket immunity the moment a firm can demonstrate sufficient legitimate use, completely ignoring any possibility that

---

106 While this Article was in the midst of publication, the Supreme Court granted certiorari in *Grokster. See* MGM Studios, Inc. v. Grokster Ltd., 125 S. Ct. 686 (2004). Andrew Rosenfield and I in response decided to develop the arguments sketched here into a full amicus brief, which ultimately was filed as *Brief of Kenneth J. Arrow, Ian Ayres, Gary Becker, William M. Landes, Steven Levitt, Douglas Lichtman, Kevin Murphy, Randal Picker, Andrew Rosenfield, and Steven Shavell, as Amici Curiae in Support of Petitioners*, MGM Studios, Inc. v. Grokster Ltd., No. 04-480 (US Sup Ct filed January 24, 2005). As we write there, the brief offers

> analysis along two dimensions. First, we summarize the economics of indirect liability, emphasizing the conditions under which indirect liability is an efficient mechanism by which to enforce the law. The thrust of this discussion is to show that the courts below have ignored many of these considerations, allowing oft-repeated but imperfect legal formulations to drown out meaningful analysis of the issues. Second, we consider specifically the liability rule adopted by both courts below and argue that it is inefficient for two reasons, but most importantly because it fails to give manufacturers any incentive to deter infringement even in instances where deterrence could be accomplished at low cost and without any significant interference with non-infringing uses.

Id. at *3.

107 Sony, 464 U.S. at 442.

108 *See* Lichtman & Landes, *supra* note 103, at 400-01, 404-07. *But see* Lemley & Reese, *supra* note 89, at 1389 n.171 (agreeing that these various issues must be considered, but expressing doubt that courts can establish a standard or presumptions that would adequately account for them).

109 This is especially true given that any technology that fails a generous cost/benefit analysis—say, a technology where current and foreseeable beneficial uses are utterly dwarfed by current and foreseeable copyright harms—would not be "banned" or banished from the field. Its inventors would still be allowed to tinker with the technology in a research setting and talk about it with other interested technologists. They simply would face liability if they chose to distribute the technology in the mass market. Courts should not be overly cautious when it comes to announcing that a particular technology causes so much harm, and offers so little benefit, that its public unveiling ought to be delayed until the tradeoff can be made more attractive, for example by identifying new non-infringing uses or by increasing the technology's ability to detect and deter infringing acts.

the firm could have done better. An analogous approach in criminal law would be to announce that anyone who does two good deeds in the morning is free to commit any number of bad acts in the afternoon. Such a rule is ridiculous because it does nothing to discourage afternoon malfeasance; but the *Sony* rule does exactly that with respect to infringement. Again, there are admittedly reasons not to be too aggressive in terms of allowing courts to micro-manage the development of new technologies. The *Sony* rule, however, has been read to contemplate no court evaluation at all. Just as courts are able to evaluate the complicated technology issues that arise in the context of the patent system,[110] and courts are able to evaluate questions of product design in the context of products liability litigation,[111] courts working in the copyright setting could be expected to evaluate whether technology firms were (say) reckless in their failure to adopt additional copyright protections. This is therefore a second dimension along which a literal reading of the *Sony* rule seems overly cautious.[112]

Issues left unresolved in *Sony* raise similar complexities. Consider, for example, the question of which legitimate uses should count as "substantial non-infringing uses" for the purposes of the *Sony* balance. Courts thus far have considered proposed uses in isolation, rather than evaluating them in light of substitute mechanisms that might allow the same beneficial use but not cause the associated copyright harm. That is in my view a significant mistake. Consider, for example, the Bible. Peer-to-peer technology could in theory be used to disseminate copies of the Bible. That would be lawful, as there is no copyright in the Bible; however, because there are already so many legitimate ways to acquire a copy of the Bible—dozens of websites post free copies online, religious institutions in every community offer free copies in print, and so on—the marginal value of additionally making the Bible available via peer-to-peer transfer is quite low. To label this a "substantial" non-infringing use is to overweight its beneficial consequences; the right approach is to evaluate substantiality in light of the next-best legally permissible approach.

This argument in fact calls into question many of the supposed "substantial non-infringing uses" that are typically identified by proponents of peer-to-peer technology. For example, peer-to-peer technology is hard to

---

110 *See generally* Arti K. Rai, *Specialized Trial Courts: Concentrating Expertise on Fact*, 17 BERKELEY TECH. L.J. 877 (2002) (discussing structural solutions to the problem of scientific complexity in patent cases).

111 *See, e.g.*, RESTATEMENT (THIRD) OF TORTS at § 2(b) (a product "is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller").

112 More concretely, why not require that firms involved with peer-to-peer software assist copyright holders in deploying decoy files? The firms might be required to use idle cycles on their servers to dish out fake files. The firms might in addition be forbidden from taking steps to interfere with decoys. Again, the *Sony* rule as interpreted today does not allow courts to even think in these directions, and that seems hard to defend. *See* Lichtman & Landes, *supra* note 103, at 400-01, 404-07.

defend on the ground that it helps strangers recommend new music one to another, because the closest substitute—a system that allows strangers to make suggestions one to another but without actually offering each other copies of the music files—makes possible almost all of the benefit but with none of the harm. Similarly, the argument about new artists using peer-to-peer technology to introduce their work must be received skeptically, given that free centralized websites (like the original mp3.com[113]) can easily be used as repositories for music that is willingly placed in the public domain. Phrased another way, a legitimate use must be evaluated in light of plausible alternative means to accomplish the same end result. This is an important detail left unmentioned in the *Sony* decision, and a detail that the appellate courts also seem to have thus far overlooked.[114]

As for still other responses to the various self-help technologies that facilitate consumer infringement, federal law offers a potpourri of approaches. One provision of the Digital Millennium Copyright Act encourages Internet service providers to remove allegedly infringing content by immunizing service providers from liability for wrongful removals made in good faith.[115] Another provision immunizes from copyright liability search engines like Google and Internet intermediaries like eBay, but only on the condition that they act expeditiously to remove infringing content from their sites the moment they are made aware of its existence.[116] Yet another forbids any firm from manufacturing, importing, or in other ways offering to the public any technology that is primarily designed to break an encryption scheme that would otherwise protect copyrighted work from unauthorized distribution.[117] Even the Federal Communications Commission has tried its hand at protecting copyrighted work; the Commission recently promulgated a series of regulations that require manufacturers of television and cable hardware to build into their equipment certain technologies that restrict the unauthorized redistribution of copyrighted television content.[118]

---

113 *See* Keith L. Alexander, *Music firm Mp3.com hits IPO high note*, USA TODAY, July 21, 1999, at 3B (reporting on the website's success as a forum for unknown artists to unveil their work). Unfortunately, this particular website lost significant ground when it changed focus and began to offer music management services that were ultimately found to infringe copyright. *See* Christopher Grimes, *MP3.com will pay Dollars 53m to Universal*, FINANCIAL TIMES, Nov. 15, 2000, at 21 (discussing litigation and settlement).

114 *See* Grokster, *supra* note 101, at 16 (counting as a legitimate use the authorized distribution of music from the band Wilco, without even considering Wilco's next-best options for online distribution). The Seventh Circuit attempted to add teeth to the term "legitimate use" in another way: that court demanded a threshold showing of current, actual legitimate uses before being willing to entertain stories of hypothetical future legitimate uses. *See* Aimster, 334 F.3d at 652-53.

115 17 U.S.C. § 512(g)(1) (2004).

116 17 U.S.C. § 512(c)(1), (d)(1), (d)(3) (2004).

117 17 U.S.C. § 1201(a)(2), (b)(1) (2004).

118 *See* Implementation of Section 304 of the Telecommunications Act of 1996, 18 F.C.C.R. 20885 (2003) (copy controls for cable television hardware); Digital Broadcast Content Protection, 18 F.C.C.R. 23550 (2003) ("broadcast flag" for broadcast content).

All of these strategies have advantages and drawbacks.[119] What is interesting about them, however, is their sheer diversity. Because consumers have this new ability to assert unilaterally the power to duplicate and distribute copyrighted work online, copyright law has had to fight back by: using immunities to entice various parties to do their part in enforcing the law; banning some technologies even though those technologies might have substantial legitimate uses;[120] and imposing by regulation specific design requirements for the next generation of television equipment. And, because all this is only working so well, there are proposals on the table to do still more—such as permitting copyright holders to engage in otherwise-illegal denial-of-service attacks as a means by which to bring down servers that are distributing copyrighted work illegally,[121] and authorizing copyright holders to unleash self-help computer viruses that would detect and destroy copyrighted music that is being offered for free by unauthorized sources.[122] In short, copyright law—perhaps more than any other field of law—has been and continues to be under enormous pressure to react to self-help measures.

IV. PATENT NONUSE

Suppose that a burglar were to invent and patent an effective home security system, but then refuse to license the technology to others (or to sell it himself) because security systems interfere with burglary. If an another inventor were to come up with the same system, should courts enforce the patent and thus bar the second inventor from making, using, or selling the

---

119 The ban on the sale of anti-circumvention devices, for example, likely has significantly reduced piracy by making it more difficult for the average consumer to acquire decryption tools. At the same time, however, the ban sweeps broadly, keeping off the market tools that have substantial legitimate uses. Worse, the ban has introduced opportunities for abuse, as where a manufacturer of remote-control garage door openers endeavored to use the provision to stop rival firms from making competing, compatible remote control devices. *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004). Whatever one thinks about the merits of that dispute—whether there should be competition for the provision of remote control devices that work with garage door openers or instead those devices should be sold exclusively by the firm that manufacturers the relevant garage door opener—it is clear that the Digital Millennium Copyright Act was not designed to address that issue.

120 The Digital Millennium Copyright Act bans technologies "primarily designed" for circumvention, with "only limited commercially significant purpose" other than circumvention, or "marketed . . . for use in" circumvention (17 U.S.C. § 1201(a)(2) (2004)), whereas the *Sony* standard more generously immunizes any technology that is "capable of substantial noninfringing uses." Sony, 464 U.S. at 442.

121 *See* Chris Marlowe, *California Congressman Backs Illegal Anti-Piracy Tactics*, HOLLYWOOD REP., June 27, 2002 (reporting Representative Howard Berman's proposal to legalize, among other tactics, the strategy of flooding computers engaged in unauthorized file swapping with large numbers of disingenuous file requests).

122 *See* Crystal Yednak, *Retribution Technology*, CHI. TRIB., June 19, 2003, at 3 (discussing proposal by Senator Orrin Hatch to allow copyright holders to use viruses to destroy files and computers involved in unauthorized file sharing). I discuss proposals like this in greater detail *infra* Part IV.

security system; or on these facts should a court refuse to enforce the patent because to enforce it would be to indirectly facilitate the illegal act of burglary? More broadly, should a patent holder be permitted to use the patent system to suppress a self-help technology where there is evidence that the patent holder is motivated by a desire to profit from the very illegal activity that the self-help technology would otherwise combat?

The above is obviously a hypothetical, but the fact pattern is not so far-fetched. In my earlier discussions,[123] I introduced the idea of using decoy files to interfere with the unauthorized distribution of copyrighted music online. Again, the intuition is that copyright holders can infiltrate a file-sharing network like Grokster, offer up mislabeled or corrupted music files, and in that way trick users into downloading undesirable songs. A college student searching for the latest Madonna tune might by virtue of this strategy accidentally download Kenny G; and, if that pattern were to repeat with sufficient frequency, the net effect would be to make illegal music significantly less attractive at the margin. What I did not mention is that there are patents that purport to cover the implementation of this strategy.[124] What would happen if a firm with financial ties to Grokster or KaZaA were to come into possession of those patents? Is this the burglar hypothetical actually realized?[125]

Patent holders in general are under no obligation to make, use, or sell their patented inventions,[126] and many patent holders in fact opt to hold even valuable inventions idle for strategic reasons. Stuart Newman, for example, is currently involved in a high-profile fight to patent the first human/animal chimera. He is pursuing the patent because he has a moral objection to this line of research and wants to use the patent to stop others from investigating these hybrids for the duration of his exclusive rights.[127]

---

123 *See supra* note 56 and accompanying text.

124 *See, e.g.*, U.S. Patent No. 5,978,791 (issued Nov. 2, 1999) (a mechanism for uniquely identifying digital files); U.S. Patent No. 6,732,180 (issued May 4, 2004) (covering the strategy of increasing or decreasing the number of decoy files available in response to current network conditions). My own suspicion is that each of these patents will be found obvious in light of prior art to which the relevant patent examiners did not have access.

125 There is reason to believe that this scenario is in fact playing out right now in the federal courts. *See* Jon Healey, *RIAA Is Accused of Patent Violations*, L.A. TIMES, Sept. 9, 2004, at C3 (reporting the filing of a patent infringement suit by Altnet against several firms that allegedly employ the decoy strategy; Altnet has a longstanding business relationship with KaZaA).

126 *See, e.g.*, Cont'l Paper Bag Co. v. E. Paper Bag Co., 210 U.S. 405, 429 (1908) ("exclusion may be . . . the very essence of the right conferred by the patent, as it is the privilege of any owner of property to use or not use it, without question of motive").

127 *See* Mark Dowie, *Talking Apes, Flying Pigs, Superhumans with Armadillo Attributes, and Other Strange Considerations of Dr. Stuart Newman's Fight to Patent a Human/Animal Chimera*, MOTHER JONES (Jan-Feb 2004) at 47. The idea of a private party using the law to impose his moral or political judgments on others is not unique to patent law. Consider tradable emission credits. Environmental groups and other interested parties can compete with firms to purchase these credits but then retire them; the effect is to reduce the maximum level of pollution from that which the law originally

Similarly, in the 1960s, the Liggett & Myers Company suppressed a patented cigarette that was arguably less carcinogenic than contemporary alternatives. The firm was apparently concerned that the existence of a safer cigarette would call into question the safety of cigarettes more generally, sharply reducing industry profits.[128] Technology firms also routinely acquire and then suppress patents on technologies that are closely related to their existing products. The motivation in these cases is to preserve demand by stopping competitors from inventing and marketing substitute goods.[129] Courts forbid none of these strategies; and that might suggest that our burglar should similarly be free to withhold his security system from the market.

Nevertheless, consider some analogies from outside patent law. A mugger cannot come to court and complain that his would-be victim used force to resist the mugging, even though the use of force is in most settings clearly prohibited. The privilege of self-defense removes the specter of liability in such an instance, because on policy grounds society long ago decided that, in certain circumstances, victims should be allowed to answer aggression with aggression. The self-defense privilege is highly fact-specific. It immunizes only those responses that are necessary to avoid imminent physical harm;[130] it extends only to responses that are proportionate to whatever harm the victim is seeking to avoid;[131] and it is fully lost if the victim fails to exhaust all "reasonably safe means of preventing" the original aggression.[132] But the privilege makes clear that, while the use of force is in general frowned upon, there are instances where force is a socially justified self-help response. Without such a privilege, an absurd result would obtain: criminal law would facilitate violent attacks by discouraging violent responses.

---

contemplated to some lower level. *See* James C. Nicholas & Julian Conrad Juergensmeyer, *Market Based Approaches to Environmental Preservation: To Environmental Mitigation Fees and Beyond*, 43 NAT. RESOURCES J. 837, 848-51 (2003). On the general question of when a private party can unilaterally decide to remove a resource from public use, *see* Lior Jacob Strahilevitz, The Right to Destroy, 114 YALE L. J. (forthcoming 2005).

128 *See* Kurt M. Saunders, *Patent Nonuse and the Role of Public Interest as a Deterrent to Technology Suppression*, 15 HARV. J. LAW & TECH 389, 393 (2002).

129 *See* Saunders, *supra* note 128, at 409-417 (offering several historical examples). This practice is arguably consistent with patent law's general goal of encouraging innovation. By allowing firms to build a fence around their original products, the patent system increases the value of those original products and thus increases the ex ante incentive to invest in their development. Indeed, the policy arguments for and against this practice largely mirror the arguments for and against awarding broad patent rights in the first place.

130 RESTATEMENT (SECOND) OF TORTS § 63(1).

131 *Id.* § 63 cmt. j.

132 *Id.* § 63 cmt. l. Interestingly, there is no obligation to retreat, nor to comply "with a command with which the actor is under no duty to comply or which the other is not privileged to enforce by the means threatened." *Id.* § 63(2).

The Digital Millennium Copyright Act provides another example on theme. A website owner who posts on his website what seem to be infringing materials cannot complain if, upon noticing those materials, an Internet service provider chooses to disable access to the site. The reason is a provision of the Digital Millennium Copyright Act that immunizes Internet service providers from "any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing . . . regardless of whether the material or activity is ultimately determined to be infringing."[133] Unlike the more nuanced self-defense privilege, in this case legal liability is brushed aside upon a mere showing of good faith. That standard is much easier to meet than the negligence standard that would apply were the service provider sued for its actions under a theory like (say) tortuous interference with a business relationship. But the lower standard is arguably justified in this instance for two reasons. First, there is not a strong need for legal liability in this setting, because Internet subscribers can discipline service providers that disable content needlessly, specifically by changing providers.[134] Second, even with immunity, there is little risk that service providers will impose substantial harm, the reason being that the statute goes on to carefully articulate several next steps for an Internet service provider to take, requiring (among other things) that the service provider notify the party whose content has been removed[135] and reestablish access to the material in approximately ten business days if the implicated copyright holder has not in that time successfully petitioned a court for injunctive relief.[136]

Even contract law has safety valves that would likely be applicable in situations where the only plausible purpose of a contractual provision is to interfere with self-help and thereby indirectly facilitate illegal activity. For instance, Sharman Networks—the firm responsible for the peer-to-peer software, KaZaA—includes in its standard software license a term that explicitly forbids users from intentionally uploading "spoofed files or files with information designed to misidentify the actual content of the file."[137] But does anyone really believe that a court would enforce that provision against a copyright holder who downloads the KaZaA software and then violates the license by posting decoy files designed to stop users from infringing that author's copyrighted works?[138] The provision would in that

---

133 17 U.S.C. § 512(g)(1).

134 Although there are many externalities at play, and thus the market is not a perfect check on Internet service provider behavior. *See generally* Lichtman & Posner, *supra* note 73.

135 17 U.S.C. § 512(g)(2)(A) (2004).

136 *Id.* at § 512(g)(2)(C).

137 Kazaa End User License Agreement 2.15, *at* http://www.kazaa.com/us/terms2.htm (last visited December 15, 2004).

138 Sharman has in fact filed suit on exactly this theory. *See* Jon Healey, *Kazaa Owner Cleared to Sue Record Labels, Movie Studios*, L.A. TIMES, Jan. 23, 2004, at C1 (reporting status of litigation between Sharman and the Recording Industry Association of America).

setting surely be void as against public policy; there is no legitimate reason for Sharman to object to decoy files as long as those files do not substantially interfere with legitimate file exchange.[139]

Copyright holders have in recent years lobbied for additional immunities along these lines, although the proposals have all been controversial.[140] For example, under current law, it is illegal to "knowingly [cause] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally [cause] damage without authorization"[141] to a computer "used in interstate or foreign commerce or communication"[142] where the damage represents a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[143] Because of this law, a copyright holder who identifies a server engaged in unauthorized file sharing might not be allowed to interfere with the server by flooding it with disingenuous download requests. Those requests would arguably "intentionally [cause] damage without authorization" and that damage would be actionable if its economic consequence were to reach the statutory threshold.

But perhaps this is a form of self-help that ought to be condoned. Residual liability—for instance, the obligation to pay for injuries caused in instances where it is later shown that the network being targeted was actually being used for predominantly legitimate purposes—could be used to encourage due care. In fact, copyright holders could be required to post a bond before engaging in this kind of denial-of-service attack, thereby ensuring that cash would be available in the event of a court-ordered payment.[144] Crafted in this manner, a balanced partial immunity might be an attractive mechanism by which to empower copyright holders to defend their own interests. There are admittedly substantial costs to weigh; immunity would exacerbate the arms race between copyright holders and infringers, and even good faith efforts will inevitably impose at least some uncompensated harm on innocent parties. But self-help in this setting is attractive both because it is flexible enough to quickly react to a changing threat landscape,

---

139 *See* Interface Group-Nevada, Inc., v. Trans World Airlines, Inc., 145 F.3d 124,135 (3rd Cir. 1998) ("Contracts that are void as against public policy are unenforceable regardless of how freely and willingly they were entered into."); RESTATEMENT (SECOND) OF CONTRACTS, § 8 (Introductory Note, 1981) (sometimes courts will refuse to enforce a contract because doing so would be "an inappropriate use of the judicial process in carrying out an unsavory transaction").

140 I briefly mentioned two of these proposals, see *supra* notes 121-122 and accompanying text.

141 18 U.S.C. § 1030(a)(5)(A)(1) (2004).

142 *Id.* at § 1030(e)(2)(B).

143 18 U.S.C. § 1030(a)(5)(B)(i) (2004). Other qualifying harms include physical harms and threats to public health or safety. Id. § 1030(a)(5)(B)(i)-(v).

144 The Berman proposal took steps in this direction, specifically by proposing that copyright holders be required to notify the Department of Justice prior to engaging in self-help, and that they be liable for damage caused to legitimate interests. *See* Beth A. Thomas, *Solutions are on Track: Digital File Sharing Spun in a Positive Light*, 6 VAND. J. ENT. L. & PRAC. 129, 134 (2003).

and because it can be designed with considerable nuance—for example, flooding a network with decoys only when the number of illegal files exceeds a certain threshold, and automatically scaling back the decoy effort as soon as the illegal behavior recedes. An absolute ban on this style of defensive measure mistakenly treats a valuable form of self-help as on par with purely wasteful forms of Internet mischief.[145]

Return now to my patent law examples, and the question of whether patent law presents issues that are meaningfully different from those presented in the contract, tort, and criminal law settings. One difference might be that there are stronger checks on patent misbehavior. My burglar, for example, might be reluctant to patent his new security system because the very act of disclosing the idea in a patent application might prompt other inventors to come up with comparable or better systems that fall outside the scope of the patent. The burglar on this story would be better off keeping his technology quiet. On the opposite story, too, the patent system seems to fare well: if the security system turns out to be so revolutionary that other inventors are not able to come up with effective substitutes even after reading the patent disclosure, then the patent should create a huge incentive for the burglar to change occupations and start selling home security. After all, on those facts, the patented technology is likely worth a fortune.[146]

Then again, maybe these arguments are not as compelling as they at first appear. With respect to the risk of disclosure, the information available on the face of a patent document is rarely revealing. As a frustrated Supreme Court once expressed, patent applicants have over time mastered "the highly developed art of drafting patent [disclosures] so that they disclose as little useful information as possible" and, thus, any "argument based upon the virtue of disclosure must be warily evaluated."[147] I do not mean to imply here that the patent system does not encourage disclosure in a typical case. Of course it does. Where an inventor is interested in profiting from his invention, a patent removes the worry that the idea will be stolen and thus frees the inventor to scream his idea from the mountaintops. In an instance where an inventor hopes to suppress his invention, however, dynamic disclosure of this sort will not occur, and in those cases the patent system is likely not particularly effective at disseminating information. It is therefore probably wrong to think that our burglar would be reluctant to

---

145 I should say that I myself prefer decoy strategies to these denial-of-service approaches, and I would only favor the latter strategy if it turns out that decoys are ineffective. My preference stems from the elegance of the decoy strategy: decoys interfere with infringing files but are unlikely to interfere much with legitimate downloading activities.

146 The social costs of burglary can also be addressed by ramping up efforts to catch and punish burglars. I do not mention that limitation in the text because it is not a consideration unique to the patent system. The same point argues against the privilege against self-defense, the immunity offered to Internet service providers, and so on. In every instance, it is obviously true that the relevant self-help technique would be unnecessary if the underlying legal rule could be enforced more aggressively.

147 Brenner v. Manson, 383 U.S. 519, 534 (1966).

patent his new security system for fear that the act of disclosing the idea in a patent application will inspire competing inventions.

As for my argument related to the value of the patent, meanwhile, there admittedly is some price at which the burglar would sell his patent to a group of concerned homeowners or himself begin marketing the technology, and thus a state of affairs where the burglar is still suppressing the technology might merely be evidence that homeowners have yet to offer an adequate sum. But it is not entirely clear that allowing this type of ransom payment is good policy, because it in essence puts law up for auction. Consider the patents related to music decoys. If infringers end up being willing to pay more for those patents, infringement will continue; if copyright holders are willing to pay more, infringement will stop. But copyright law must promise more to authors than merely the right to participate in an auction where the winner decides whether copyright is respected or ignored.

In the end, the right answer here will largely turn on whether courts can predictably and accurately exercise discretion in cases like the burglar hypothetical. Courts would need to be able to distinguish instances where a patent holder is attempting to profit from the patented invention, which presumably should be allowed, from instances where a patent holder is instead attempting to protect profits that derive from some underlying illegal act, which probably should not be. That is, a court should enforce a patent where the patent holder developed an innovative self-help mechanism, patented it, and is now using that technique or trying to license others to do so. In such a case, the patent system is serving its traditional role of encouraging innovation by creating an exclusive right to make, use, or sell an original invention. But a court should at least hesitate in an instance where the patent holder has developed an innovative self-help mechanism, patented it, and is now refusing to use or license that invention. This is not to say that refusals to use or license are always illegitimate. As I mentioned, a patent holder might be keeping one patent off the market in order to increase the value of another, or intentionally retiring a technology to which the patent holder has a moral objection. But such refusals should at a minimum be viewed with skepticism where they are motivated by a desire to profit from the very illegal activity that the patented self-help technique would combat. Under that fact pattern, the patent is at best only weakly serving the patent system's traditional goals of encouraging the development and dissemination of new technologies. Thus, if society is sincere in its characterization of the underlying act as illegal, and if society has confidence that these cases can be reliably distinguished from other instances of patent nonuse—and that latter "if" is admittedly a big one—courts arguably can[148] and likely should[149] refuse to enforce any implicated patents.

---

148 *See, e.g.*, Keystone Driller Co. v. General Excavator Co., 290 U.S. 240, 245 (1933) (reaffirming, in the context of a patent dispute, the equitable principle that "whenever a party who, as actor, seeks to set the judicial machinery in motion and obtain some remedy, has violated conscience, or good faith,

V. CONCLUSION

The theme of this conference is that technology brings a new urgency to the question of how legal rules account for and respond to private self-help mechanisms. The link is not only that technology creates new opportunities for self-help—think here of encryption serving to increase a copyright holder's ability to control his work, or Internet filters arming consumers with new tools against offensive communications online—but also that technology expands the need for self-help, primarily because formal legal rules will often prove too slow to respond to emerging technological threats. My purpose in this Essay was to present some case studies that shed light on the issues that these new technologies will raise, specifically by highlighting and evaluating the ways in which legal rules encourage, harness, deter and indeed defer to self-help.

The primary payoff to this work, in my view, is that these several case studies make clear the rich variety of options available, from supportive approaches that cast self-help as a necessary prerequisite to more formal legal process—for example the rule in trade secret law that protects secrets only if they were revealed despite reasonable self-help precautions—to less welcoming alternatives, like the copyright doctrine that forces authors to choose between encryption and copyright, rather than allowing an author to rely simultaneously on both. As my discussions have emphasized, the theories that underlie these approaches vary considerably. Thus, the task of choosing the right approach for a particular setting in the end requires a careful look at that specific application, rather than any generic rule that might apply across the board. This is in fact the main reason why I was in this Essay attracted to the case study approach. In my view, it is only by delving into each particular example that one can really understand what work self-help can accomplish, and what instead is best left for government actors and institutions.

---

or other equitable principle, in his prior conduct, then the doors of the court will be shut against him in limine; the court will refuse to interfere on his behalf, to acknowledge his right, or to award him any remedy") (quoting POMEROY, EQUITY JURISPRUDENCE, 4th ed., § 397); Morton Salt Co. v. G. S. Suppiger Co., 314 U.S. 488, 494 (1942) ("The patentee . . . may not claim protection of his grant by the courts where it is being used to subvert [public] policy.").

[149] Note that there are several plausible approaches that are less severe than a complete refusal to enforce a suspect patent. For example, a court could impose a reasonable royalty. Or, if the courts are unable to make these determinations with sufficient accuracy, the government could condemn particularly troubling patents and then offer fair compensation. These more forgiving approaches reduce the importance of mistakes in that they offer the patent holder at least some financial reward, rather than turning the patent holder away empty-handed.

BOOK REVIEW

Niva Elkin-Koren and Eli M. Salzberger, *Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law* (2004).

One of the interesting – and frustrating – delays in moving any field to a new level is that challenging ourselves to generate more advanced frames of reference is difficult. Wrapping our minds around developing issues with no existing constructs takes time. The delay is inevitable, and yet aggravating to the large group of practitioners awaiting an end to uncertainty so they can develop effective tools to use and apply. The first step in making the intellectual leap is to achieve recognition among some group of thinkers that existing tools are inadequate. The first evolutionary strides, in other words, involve a period in which productivity centers on identifying problems, or sets of problems, that require attention. To the outsider, this looks like empty rhetoric and unnecessary delay. Insiders – those struggling with the problems – know it is an essential part of the process.

Early in the history of cyberspace, we went through such a period. The first writing about cyberspace and the law was characterized by a tone of high-stress reaction, throughout which ran the theme of novelty: cyberspace is so new and different that we don't know how to think about it; no existing law applies. It must require an entirely new body of law and analysis to be developed.

After a few years, a counter-trend emerged: many commentators asserted that there is nothing new under the sun (or in cyberspace). Legal problems presented by cyberspace can be addressed in the way legal problems have always been addressed – namely, by adapting existing legal arguments and frameworks to new circumstances through analogy and logic.

Now, perhaps, we are reaching a new level of subtlety in our discourse. We can acknowledge that many of the problems posed by the Internet are similar to those in realspace. Contract law still applies, for instance, and certain details of contract law have been adapted to the new parameters of remote consent. "Signatures" can be translated into digital equivalents. Records can be kept and shared according to existing legal frameworks. Examples of the expansion of legal paradigms into cyberspace are now common.

Yet as we strike out the easy problems, a new set is becoming clearer. Another delay ensues as we pause to define them. By pushing the boundaries of existing legal frameworks, we can begin to see where they fail. And here is where the problems get interesting – where, perhaps, the elusive field of "cyberlaw" begins to come of age.

Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law is, in many ways, the ideal "prequel" to this issue of *The Journal of Law, Economics and Policy* on cybersecurity and self-help. Niva Elkin-Koren and Eli M. Salzberger set out a concise history

of three generations in the Law and Economics movement. They describe the Chicago School, move through Coasian development (Transaction Cost Analysis), and define Neoinstitutional Law and Economics as the current, or latest, form of the analytical approach.

Elkin-Koren and Salzberger carefully and methodically summarize the characteristics of each stage of the movement, first explaining the novel insight that led to the adoption of the approach and describing the analytical leaps that the insight made possible. They follow by demonstrating the analytical weaknesses that gave rise to the foundational insights of each follow-on movement.

Now, the authors observe, we may have reached another takeoff point. In several areas, existing law and economic models fail due to incorrect or inadequate assumption sets. While the Chicago School, Transaction Cost Analysis, and Neoinstitutional Analysis all bring tools to the table, they have a common denominator when applied to cyberspace: they all appear to indicate a decline of market failures. A decline in market failures, in turn, would support a policy of less central, or governmental, intervention.

Elkin-Koren and Salzberger highlight this common conclusion because, as they persuasively argue, it demonstrates the limitations of existing Law and Economics tools when applied to cyberspace. Despite the range of thinking and the variety of analyses that Law and Economics makes possible, it is still not broad enough (or mature enough?) to adequately guide policymakers seeking to manage cyberspace effectively.

The authors offer several examples that support their assertion. One of the most compelling is also the most complex. Their discussion of legal and institutional norms begins to point to the need for multidimensional structures describing cyberspace. Kelsen's 1949 pyramid of norms, based upon a pyramid of institutions, has provided a common descriptive framework for parliamentary democracy in legal literature for decades. Legal norms, in this standard view, derive from social consensus about a higher set of values, which are themselves reflected in institutions. Legal norms, as the representation of the norms collectively reflected in institutions, have enhanced legitimacy as the governing social norm.

The Kelsen assumptions about norms do not hold sway in cyberspace for at least three reasons. First, although the authors do not focus here, cyberspace does not obey our assumptions about jurisdiction. In other words, even if societies operated according to Kelsen's pyramid, cyberspace inhabits too many pyramids for the analysis to remain valid. Second (and the authors' primary point), cyberspace reduces the costs of collective action, thereby creating a bottom-up set of norms in the cyber-environment – directly contrary to the law-as-ultimate-arbiter norm in realspace. Third, it is possible that cyberspace actually generates entirely new sources of "law" (or its equivalent). Elkin-Koren and Salzberger bring in the now-famous Lessig argument that code *is* law. If true (this observer thinks it often is)

this new source of authority has untold ramifications for both law and economic study.

In the end, *Law, Economics and Cyberspace* is both an essential and a frustrating step on the road to a new model for cyberspace. Identifying problems is a step toward solving them. But this panoply of the unaddressed is tantalizingly open-ended. It will be years before we can wrap our minds around the analytical gaps that Elkin-Koren and Salzberger describe. In the meantime, cyberspace – always a moving target – will itself have evolved to new heights.

Emily Frye[*]

[*] Associate Director of Law and Economics Programs at the Critical Infrastructure Protection Project (CIP Project).

BOOK REVIEW

Lawrence Lessig, *Free Culture—How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (2004).

Free Culture by Lawrence Lessig is a response to recent statutory and judicial developments in the area of intellectual property (IP), against the background of the technological revolution of the Internet. Lessig criticizes the path of these developments, arguing forcefully that the legislature and the courts have surrendered to big media and to powerful interest groups, thereby enhancing the scope of intellectual property, shrinking the public domain, increasing control of creativity, and posing a serious threat to free culture—all this in sharp contrast to American tradition. The book is written to the broad intelligent audience, but it is by no means simplistic or shallow. It contains numerous interesting insights, analytical arguments, historical accounts and personal stories, which crystallize together into a coherent voice not heard loud enough, so far, beyond the academic circles. It does not provide a technical Law and Economics analysis, but it does contain important insights that can be (and ought to be) re-structured within this discipline.

I. POSITIVE ANALYSIS

The Statute of Ann (1710), which created a statutory copyright in England, is considered to be the first legislation in the area of intellectual property. Lessig shows us (Ch. 6), in contrast to conventional wisdom, that this statute, as well as Article I, section 8 of the U.S. Constitution (the Progress Clause) was meant to narrow existing intellectual property rights, which were developed by the common law. Law and Economics scholars often point to the efficiency of the common law as opposed to legislation. Lessig's historical account of courts' handling of intellectual property does not lend support to this argument.

Nevertheless, from this 18th century starting point, the legislature took a one-way route towards a constant expansion of copyright: in duration - from 14 years plus 14 years optional extension in 1790 to 95 years in 1998; in scope—from books, maps and charts in 1790 to the inclusion of music, software and architecture today; from exclusive power to publish to exclusive power to exercise control over any copy of the creation; from protection of the particular work created to protection which includes any derivative work; and in procedure—from a demand of registration and a deposit of copy, to automatic creation of rights. Similar trends characterize other intellectual property rights, such as patents and trademarks.

This expansion of intellectual property rights, as shown by Lessig through fascinating particular stories from the past two hundred years, was

not the result of a systematic normative thinking, but the result of pressure by interest groups, and of the changing nature of the relevant markets (e.g., the publishing, entertainment, and pharmaceutical industries), which became more concentrated. The major players became more powerful and thus could apply growing pressure on the legislature. The positive analysis of intellectual property indeed conforms to basic Public Choice insights regarding legislation. Lessig's account of the development of intellectual property flatters neither the legislature, nor the courts.

II. NORMATIVE ANALYSIS AND THE LAW AND ECONOMICS PARADIGM

Lessig is neither an anarchist nor an enemy of intellectual property. He advocates, though, a more balanced approach to defining the scope of intellectual property. Although he does not make this explicit, Lessig, in fact, adopts the basic Law and Economics rationale for IP. This rationale and the tools to achieve it are somewhat confusing within the Law and Economics paradigm itself. Two points in this context should exemplify this statement. First, economists generally favor free markets over government regulation, but in the context of intellectual property it is not clear whether creating or broadening intellectual property rights through law are on the side of free markets or government intervention. On the one hand, the main tool to create intangible property is the law; hence IP is on the side of intervention in the market. On the other hand, markets can operate only on the basis of private property, or, in other words, property is a basic precondition for the market to operate; hence IP is on the side of a free market.

Second, the prime normative goal of Law and Economics is to maximize the welfare of society. Without intellectual property, incentives to create would be lacking. New drugs would not be developed, new ideas would not be published, and cultural and scientific progress would cease or significantly slow down, decreasing the welfare of society. However, most new inventions—whether scientific or cultural—are based on older ones. Full propertization of every idea and expression would thus slow down scientific and cultural progress. Lessig tells us various stories to exemplify this insight. For example, the obstacle of clearing rights prevents new creations that were meant to be based on sampling and reviving old cultural icons (Ch. 8). In order to enhance society's welfare we do need a significant public domain. Granting intellectual property rights, therefore, works both to stimulate progress and creation, on the one hand, and to slow them down, on the other. To achieve a balance, a more sophisticated framework is needed that acknowledges these disparate effects.

These two points are captured beautifully by Lessig when he explains his idea of free culture:

> A Free culture supports and protects creators and innovators. It does this directly by granting intellectual property rights. But it does so indirectly by limiting the reach of those rights, to

> guarantee that follow-on creators and innovators remain *as free as possible* from the control of the past. A free culture is not a culture without property, just as a free market is not a market in which everything is free. The opposite of free culture is a 'permission culture'- a culture in which creators get to create only with the permission of the powerful, or the creators from the past (p. xiv)

III. THE ROLE OF TECHNOLOGY IN THE CONTEXT OF THE ECONOMIC ANALYSIS OF LAW

Free Culture provides readers with illuminating stories from the history of scientific and cultural development in America in the context of existing laws, especially those of intellectual property. For example, Lessig discusses the invention of paper film for cameras by George Eastman in the context of piracy (Ch.2), the invention of the airplane by the Wright brothers and the question of vertical property rights (Introduction), and the invention of FM radio by Howard Armstrong and the attempt of RCA to block it (Introduction). The lesson from these stories is that had the law responded differently to these innovations or applied the existing legal doctrines at the time the invention was made, today we would probably be without the day-to-day usage of these inventions—no cameras, no airplanes, no FM radio.

The bulk of the book, though, is dedicated to the discussion of the same theme—the suitability of existing legal norms and the way that they are enforced in the context of the contemporary technological revolution of the Internet. The inter-relations between technology and law are a major feature illuminated in the book. Technology is a substitute for law. If one can protect tangibles or intangibles by physical or technological means, one does not need the law to grant one a property right. If, on the other hand, law provides sufficient protection, physical fences and technological barriers are unnecessary. Thus, the law also affects the course of technological developments and the direction of progress. A no less important feature of these relations is that the law, being general, has a totally different meaning and scope with every technological change.

Copyright was initially about the exclusive right to publish. Only when technological change (e.g., the invention of the photocopying machine) enabled cheap and massive copying did the scope of copyright expand. But here comes the twist: the technology of the Internet is all about copying; every operation on the Internet involves copying and is thus an infringement of copyright, at least prima facie. The law today, therefore, is too broad, and copyright has to be narrowed.

Lessig's point regarding technology in the context of intellectual property (which he analyzed also in a previous book—*Code and Other Laws of Cyberspace* 1999) is a crucial insight regarding the Law and Economics project as a whole. Indeed, the state of technology is a factor ignored so far by the most basic Law and Economics models. Consider, for example, the Coase theorem, which predicts that in a world of zero transaction costs, the

law does not matter. Market forces will lead us to efficiency regardless of who is assigned the entitlement (whether it is the factory that is entitled to pollute or the neighbors who are entitled to clean air) and the means to protect it (a property rule or a liability one). This brilliant analysis (which was expanded by Calabresi and Melamed) implicitly takes the technological state or technological frontier as given. In the old world where technological change was very slow, this might not have been a serious shortcoming of the model, but today when technological change is so rapid, the law matters even in a world with no transaction costs. Thus granting the entitlement to free air is likely to have different effects in terms of innovation to reduce pollution than granting an entitlement to pollute. We do need to endogenize technology into the basic Law and Economics analysis.

IV. TRANSACTION COSTS

Lessig's major argument is that technology unintendedly changes the effect and scope of the legal arrangement vis-à-vis the division between free culture and culture by permission. Critics may reply that "fair use" can re-balance the technological change, and obviously, if due to Internet technology every operation involves copying, then copying will not necessarily be deemed an infringement of intellectual property (because one can claim the defense of fair use.) This leads Lessig to his next argument—which, in the terminology of Law and Economics, is that of transaction costs. If the legal focus shifts to fair use, the role of litigation and lawyers increases significantly. Since people want to know their legal situation ex-ante, they will have to consult lawyers for every action in which they are engaged. (Lessig describes forcefully how the task of "clearing rights" can be a lengthy and expensive experience deterring potential creators from materializing their ideas, e.g., Ch. 8.) Creators, and especially those who are incorporated for profit, will naturally and understandably wish to increase their revenues from intellectual property by relying on the current scope of IP law.

In this context Lessig describes threats of mega lawsuits against individuals in which the potential defendants did not have the means to fight in court and thus were willing to settle for the maximum amounts they could afford to pay (e.g., the story about the Rensselaer Polytechnic Institute student told in Ch. 3). Even if fair use stands on the defendants' side, the unequal power relations mean that the law on the ground develops very differently from the law in the books. The extension of copyright periods means also that it is much more difficult to locate the owners, adding to the time and money spent ex-ante. Indeed, the current intellectual property regime increased transaction costs significantly, a fact that decreases creativity and harms cultural and scientific progress, thus diminishing society's welfare. This is another major reason for reforms.

V. REFORMS

Lessig has several proposals for reforms (Afterword). These include shortening the period of copyright so as to provide sufficient incentives to create but nothing more. This principle is right but the question remains: how long is this period, and how can this period be adjusted to changing technological developments? Other proposals are more concrete, such as the return to an initial period that can be renewed by request of the owner. A lack of such application for renewal can signal that the creation no longer has a significant economic value for its owner and thus can enter the public domain and be used freely by everyone. Another suggestion is to re-introduce registration and marking, using the new tools of the Internet to keep these formalities simple and cheap. These measures can increase information and decrease transaction costs, and thus contribute to society's welfare.

Other proposals are meant to narrow the scope of the right, distinguishing, for example, between the primary right and the derivative right, which ought to be much shorter, and between different purposes of sharing files. The law, according to Lessig, should not treat equally those who download music, using P2P technology as a substitute for purchasing a CD, and those who do the same because the content is no longer sold in the stores. The last proposal might sound right, but it could be costly to enforce. It would also increase the lawyer's role (and thus transaction costs), a feature that Lessig himself forcefully advocates against.

Lessig also advocates private action in the shadow of existing norms. He himself is the founding father of the Creative Commons project, which is a sophisticated way to use the current intellectual property regime to create a third domain, distinct from the public domain and the strict copyright domain. Individuals voluntarily place their creations in this third domain and use IP law to ensure that subsequent users and modifiers do not prevent others from free access or use (according to individual terms that every contributor can attach to the creation). Lessig's private enterprise can serve as an interesting example for the Coase theorem, which predicts that regardless of the legal arrangement, in a world with no transaction costs (and in the Internet transaction costs are indeed significantly lower), interacting individuals will bargain in the shadow of inefficient law (the current IP laws) towards an efficient equilibrium.

VI. CONCLUSION

This short essay cannot fully elaborate on all the rich content of *Free Culture*, and it even fails to provide a full synopsis. I did not mention, for example, Lessig's personal account of the Eldred case in which he made the argument before the U.S. Supreme Court on behalf of Eldred and failed,

providing a fascinating ground for additional insights not only within the Law and Economics discourse but far beyond. Many of the questions dealt with in the book, however, will get a second chance at the Supreme Court this coming term in the Grokster case, where the court will reconsider whether companies enabling P2P file sharing are liable for their users' copyright violations.

I hope that those who read this review will develop the appetite to read the book. It is indeed worthwhile.

*Eli M. Salzberger**

* Professor of Law and Vice Dean, Faculty of Law, University of Haifa, Israel.