2005

Community Self Help

Neal K. Katyal
Georgetown University Law Center, katyaln@law.georgetown.edu

1 J.L. Econ. & Pol'y 33-67 (2005)

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:

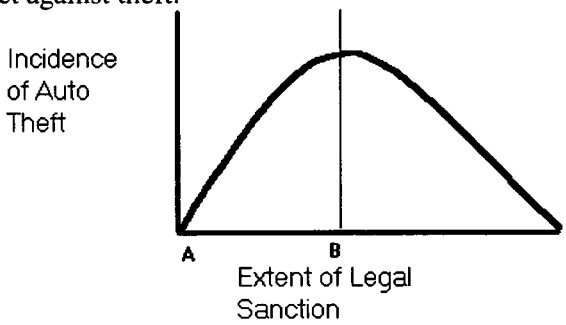
> If such withdrawal from local networks becomes widespread, the sense of mutual responsibility among the residents is undermined, and those who are able to do so may attempt to physically abandon the neighborhood at the earliest possibility. As a result, the capacity for local control may further deteriorate,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