CEI OnPoint

Competitive Enterprise Institute
1001 Connecticut Ave NW • Suite 1250 • Washington, DC 20036
202.331.1010 • www.cei.org
Advancing Liberty – From the Economy to Ecology

October 24, 2006 **No. 109**

Giving Chase in Cyberspace

Does Vigilantism Against Hackers and File-sharers Make Sense?

By Clyde Wayne Crews Jr.[*]

In the debate over identity theft and online security, commentators often note that markets and private actors are better equipped than regulators to counter cybersecurity breaches and instances of copyright infringement. This paper considers an extreme instance of cybersecurity self-help: that of attacking the attackers.

Internet vigilantes are already at work: The 419 Flash Mob, for example, works to disable and report to authorities the websites of "phishers" who trick users into entering their information on phony websites made up to look like those of real banks and merchants.[1] Recently, 419 enlisted as many Internet users as possible over a 48-hour period to launch attacks on Web servers used by criminals.

Whose Rules? Does it make sense to give chase and hack back at identity thieves and their ilk? There's both good and bad in the notion of using hackers'—and even potential cyber-terrorists'—own tools against them. This issue raises questions about government's proper role in online governance: What are property rights in online communications networks? Who gets to call the shots? Who has the right to do what? On the Internet, which has no single proprietor to set the rules of network behavior, it is often far from clear what constitutes trespass or a violation. This lack of clear authority is what has led to numerous debates over the years over pop-up ads, spam, privacy, spyware that track our online use, and more.

Given many Internet users' preference for government to keep a hands off approach, there is a natural tendency to want to solve one's own problems by giving chase. So, it is appropriate to address self-help in the light of what it means for cybersecurity and digital content protection. Is it a plus or a minus? Sometimes self-help is plainly outrageous: In

[*] Clyde Wayne Crews, Jr. is vice president for policy and director of technology studies at the Competitive Enterprise Institute.

a notorious case of “spam rage,” one man was so fed up with receiving “male enlargement” ads that he threatened to torture and kill the spammers.[2] A vastly more measured and sensible campaign is Microsoft’s $5 million Anti-Virus Reward Program, which began in 2003 by offering $250,000 bounties apiece for information leading to the convictions of the creators of the SoBig and MSBlast viruses.[3] After the MyDoom worm in January 2004, SCO Group Inc., a company targeted by the infection along with Microsoft, offered $250,000 for information leading to arrests.

The White-Hat Hacking Exception? Yes and No. Some self-appointed do-gooders, like a Los Angeles man charged with hacking into and redirecting visitors away from the Al-Jazeera television network’s website,[4] engage in “patriot hacking” by targeting websites— albeit illegally—believed to support terrorism.[5] Meanwhile, some organizations without a political agenda, but still concerned about online break-ins and theft of digital content, want the freedom to retaliate against the perceived cyber thieves and trespassers. The entertainment industry has sought legislation granting it immunity from prosecution for what some might call “hacking” into peer-to-peer (P2P) networks whereby users share files. This is a form of digital self-help, but in an age of widespread cybersecurity vulnerabilities, it’s difficult to know what to expect from governmental cybersecurity standards if the government grants immunity from liability to selected parties for damages caused by unauthorized access to personal computers at the same time that the Net is plagued by an outbreak of that very problem. How would Washington reconcile stopping break-ins while at the same time granting to some the right to break in?

In an interconnected cyberspace, seemingly mundane self-help policies can carry big implications. For example, major players can tweak one another’s software in seemingly unbecoming ways. A built-in feature of Windows that allowed technicians’ messages to appear on users’ computers in a networked office environment was being disabled by America Online’s dial-up software in order to thwart a kind of pop-up spam that was exploiting the feature. Is such a “hack” on behalf of others acceptable? As security guru Bruce Schneier of Counterpane Internet Security notes, this raises some serious concerns: “They are trying to do the right thing...but you sort of feel dirty after you hear it…It’s a very dangerous precedent in having companies go into your computer and turn things on and off…From there, it’s easy to turn off competitors’ services.”[6] In these instances, it seems the parties in question have ample incentives to resolve such questions without government getting involved. Moreover, numerous companies engage in turning off spyware, even though the creators of spyware often claim their products are downloaded only when authorized.

The openness of the Internet can make seemingly straightforward security policing more difficult. Exhibit A is the issue of appropriate defense of copyrights. Recording companies cannot break into your house and log into your computer to delete unauthorized MP3 files, nor can they sneak into your office and access the network to do the same. Into this legal environment, though, fell the “Peer-to-Peer Piracy Prevention Act,” sponsored by Rep. Howard Berman (D-Calif.). The bill, which never got out of committee but was widely reported in the media, would have given Hollywood and the music industry immunity from liability when they access peer-to-peer networks and attempt to prevent trade in their copyrighted material. In other words, the bill would “let Hollywood hack”—and the industry is bound to try again.[7]

Copyright holders’ pain is real, and their plight over lost compensation does arise from the unforeseen ease of sharing allowed by the Internet. However, granting the entertainment industry a pass to police our personal computers and future Internet devices cuts against broader cybersecurity goals, particularly since anyone claiming a copyright would then be able to indulge in such vigilantism. Private property owners have the right to defend their possessions, but they do not have a right to take damaging offensive action. Technological self-help is legitimate, but breaking and entering is not—particularly when Internet break-ins are one of today’s most vexing security problems. Under the Berman bill, copyright holders—or more likely the large movie studios and recording labels that represent them—would be granted a broad liability safe harbor to police P2P networks.

The real question over the appropriateness of such legislation is just exactly what online activities would be permissible under the exemption: Monitoring users? Sending warning notices to alleged violators? Destroying certain files on others’ machines? Sending viruses into networks? Especially given the Net’s inherent lack of security, it is unclear what legislation of this sort would unleash not only on P2P networks, but on the broader Internet, other communications systems like cell phones, and on future private networks or technologies yet to be developed.

Targeting criminals and hackers, rather than regulating computer networks on behalf of security, remains in the best interest of Internet users. Yet that is an exceedingly difficult job, evidenced by the fact that major virus authors and hackers remain at large. Given the difficulty of locating hackers, this is no time for new policies that might unintentionally *promote* hacking against targets who may not be guilty of anything.

Some self-help remedies available to content creators seem more benign than others, and appear unobjectionable. If copyright owners are simply loading up their own computer servers with harmless dummy files posing as copyrighted pop songs, no one has cause to complain when accessing those instead of a real file: There is no free entitlement to another’s copyrighted music. Attorney James DeLong, for example, has noted that if copyright owners deploy phony decoy files that began playing a song or movie—only to then launch into a scolding lecture on the evils of copyright infringement, one could hardly claim harm.[8] Such dummy files alone, which entail no intrusive access to anyone else’s computer since they are stored on one’s own machine, can help accomplish the goal of making unauthorized P2P file swapping of copyrighted materials too cumbersome and uncertain to be worth the trouble.

A widely cited study by Andrew H. Chen and Andrew M. Schroeder, two University of Washington undergraduate students, suggests that such “spoofing” techniques may work to protect content if combined with selective litigation against the most egregious file pirates.[9] Importantly, though, these sorts of self-help measures can be carried out without pro-hacking legislation. Companies like Overpeer were among those already engaged in such spoofing on behalf of industry.

Innocents in the Crossfire: You Mean I'm a Hacker? Several controversial self-help methods have arisen to combat spam. Some proposals would employ new types of email filters capable of engaging in automatic denial-of-service-style attacks against spammers' websites to raise their bandwidth costs. However, one difficulty is that many spammers hide themselves by signing up for free Web services, meaning legitimate users of the services would be impacted by the retaliatory action, too.[10] Moreover, pranksters can target legitimate companies by sending bulk emails pretending to be from those targets.[11] Nonetheless, spam has inspired legions of self-appointed, volunteer spam-busters, in part precisely because the Internet is not governable by a single authority.[12] As Jonathan Zittrain, co-founder of the Berkman Center for Internet and Society at Harvard Law School notes, "In the absence of an effective public [Internet] sheriff, you will have these private ones"[13] Lately, the arms race has escalated further: The spam busters *themselves* have become targets of denial of service attacks.[14]

Such limited success is one reason the government does not typically endorse "white hat" or "patriot" hacking against either ordinary hackers or foreign governments.[15] Like the spam busters who find themselves in the crosshairs, white hat or "ethical" hackers could be tricked and find their attack against a rival party backfiring. Nonetheless, testing of the waters will likely persist: One technique would use computers targeted but not yet infected by a worm to trace that worm, prevent its spread to other machines, and shut down, but not harm, the perpetrating computer.[16] Companies under attack by hackers will attempt to identify the perpetrator and give chase. (The military is experimenting with such platforms to address potential cyber-terrorist attacks.)[17] But, as noted, offering blanket immunity to hacker chasers could be problematic; The defender, with the best of intentions, may chase and disrupt an innocent party. Overambitious vigilantism could put innocent computer users at risk.

Self-help security operations pose another threat. "Trojan" software is so prevalent that the hacker may not even know he's a hacker. Viruses may commandeer vulnerable computers and use them to launch spam or further virus attacks, while the owners of those computers have no idea that their machines are being exploited. If an innocent individual's computer is sending out spam without that individual's knowledge, he or she is not the proper target of the white hat vigilante. The bad guys understand this weakness and can exploit it: A new wrinkle plaguing efforts to prosecute hackers, is the "Trojan defense"—aggravated by the Net's anonymous character—by which a defendant can claim that his or her computer was hijacked by another, and that that unseen other is the source of a given attack.

Honeypots and Self-Help. Despite the downsides of aggressive, well-intended white-hat hacking of others' computers, "hacking" that probes weaknesses in one's *own* network is widespread and encouraged. The federal government, for example, employs white hat hackers to test the resiliency of its computer systems. Governments and companies alike have their own security personnel trained in intensive white-hat hacking courses and seminars to enable testing of vulnerabilities in their own networks, and to experiment with responses.[18] (One proposal even suggests expanding the concept beyond the cyber sector, proposing the testing of security systems by allowing certain screened and registered white-hats to attempt to bring mock "weapons" onto planes as a means of testing the security procedures. Succeed and win a bounty of, say, $1,000; get caught, pay $1,000, part of which goes to the guards who discover the offense.[19]) The idea of internal white hat hacking is for the incentive structure to continually improve the inspection system and the network.

Patriot and white hat hacking, as well as self-help aimed at protecting digital content, are aimed at reaching *outward* to thwart a perpetrator. An alternative is setting traps on one's own turf. Michael Schrage, a senior advisor to MIT's Security Studies program, favors turning the tables on perpetrators. He invokes the importance of proactive "digital decoys" or "honeypots" to trap intruders, helping ensure that hackers can never be certain they're not being tracked as they carry out what they think to be a surreptitious invasion of a computer network. As he wrote in *The Washington Post*:[20]

> Federal agencies and Fortune 500 CIOs who don't actively use a computer cupboard full of honeypots to attract and distract hackers, network crackers and malefactors are failing to adequately protect their organizations.
>
> Technically speaking, honeypots are digital decoys designed to make intruders think they've breached an organization's real defenses. In truth, however, the intruders have entered a tightly monitored environment that tracks every illicit keystroke…
>
> Honeypots are really not about using networks to reach out and grab someone, but about deceiving those who have already decided to access something they know it is illegal or immoral for them to access.

This is a superb description of legitimate, non-intrusive self-help: Nobody gets hacked and nobody innocent gets hurt. Only the trade in copyrighted material or network hacking would be inconvenienced. With such methods, more extreme "hacking" authorization need not come from government. Record and movie companies—and the rest of us—can self-protect in ways that have no chance of impinging on third parties. P2P networks that trade in files with owners' permission, for example, would continue unimpeded. On a public Internet, where government policy is likely to be ham-handed anyway, it would be risky and cumbersome to have different "right to hack" rules apply to different classes of Internet users. It is true that we agree to share some portion of the contents of our hard drives when we make it accessible to other users on a P2P network, but the implied permission we grant stops there. It makes little sense for policy makers to explicitly authorize invasion of computer networks in the new era of concern over cybersecurity.

Conclusion: Responsibility Cuts Both Ways. Explicit liability protection for particular classes of white hat hacking is ill advised. If invaders cause damage, no matter their intention, then liability for damage they cause is usually appropriate. Special hacking rights can easily lead to collateral damage to third parties. Standards for liability will likely emerge in the cybersecurity marketplace for numerous purposes, perhaps even to protect evolving sorts of white-hat hacking that might cause potential third-party damage. Time will tell: Hackers' rights aren't being violated by stopping them. But on the other hand we cannot stop them in such a way that legitimate file-sharing users or other innocents are caught in the crossfire. A green light for hacking can work against broader cybersecurity and intellectual property goals, and there are alternatives.

Notes

[1] See Dan Ilett, "Vigilantes Launch Attack On Scam Sites," *CNET News.com*, February 10, 2005. http://news.com.com/2102-7349_3-5571061.html?tag=st.util.print.

[2] "Male Enlargement Ads Prompt Spam Rage," Reuters, *CNN*.com. November 24, 2003. http://www.cnn.com/2003/TECH/internet/11/24/spam.rage.reut/index.html.

[3] "Microsoft Announces Anti-Virus Reward Program ," Microsoft Press Release, November 5, 2003. http://www.microsoft.com/presspass/press/2003/nov03/11-05AntiVirusRewardsPR.asp. Coverage at Suzanne Goldenberg, "US Giant Puts Up $5m to Trap Hackers," *The Guardian*, November 6, 2003, http://www.soci.niu.edu/~crypt/other/bounty.htm.

[4] "Al-Jazeera Hacker Sentenced," Reutuers, *CNET News.com*, November 2003, http://news.com.com/2102-7349_3-5107409.html?tag=st_util_print.

[5] Alex Rodriguez, "Hackers Direct Their Anger Online," *Chicago Tribune*, September 27, 2001, p. 2. http://www.chicagotribune.com/news/specials/911/showcase/chi-0109270190sep27,0,4807017.story.

[6] Quoted in "AOL Quietly Changes Windows Settings to Combat Pop-Up Spam," *SiliconValley.com*, October 23, 2003. http://www.siliconvalley.com/mld/siliconvalley/7086508.htm.

[7] Phrase seen in James D. Miller, "Let Hollywood Hack," *TechCentralStation.com*, August 22, 2002. http://techcentralstation.com/082202B.html.

[8] James V. DeLong, "IP And Technological Self-Help: Barbed Wire For The Digital Age," *CEI C:\Spin*, July 2, 2002 http://www.cei.org/gencon/016,03114.cfm.

[9] Andrew H. Chen and Andrew M. Schroeder, "A Modified Depensation Model of Peer to Peer Networks: Systemic Catastrophes and other Potential Weaknesses," Universion of Washington, August 2002. http://students.washington.edu/achen/papers/p2p-paper.pdf.

[10] See Amit Asaravala, "Spam Wars: Filters Strike Back," *Wired News*, November 4, 2003. http://www.wired.com/news/business/0,1367,61012,00.html.

[11] Ibid. Asaravala, 2003.

[12] See Michael A. Hiltzik, "Lone Guns Set Sites On Spam," *Los Angeles Times*, April 16, 2001. p. A1.

[13] Hiltzik, 2001.

[14] Reuters, "New E-mail Worm Targets Antispammers," Reuters, December 3, 2003. http://news.com.com/2100-7349-5113064.html.

[15] Associated Press, "Government Warns 'Patriot Hackers' Against Cyber Attacks On Iraqi Interests," February 12, 2003. http://www.bayarea.com/mld/siliconvalley/business/special_packages/security/5166977.htm.

[16] Described in Elinor Mills Abreu, "Computers Under Attack Can Hack Back, Expert Says," *SiliconValley.com*, August 3, 2002. http://www.siliconvalley.com/mld/siliconvalley/3795332.htm.

[17] For example, see Teresa Riordan, "A Digital Architecture of Defense," *New York Times*, August 5, 2002. p. C4.

[18] Jon Swartz, "Tech Pros Get to Know Their Enemy," *USA Today*, September 23, 2003. http://www.usatoday.com/tech/news/2003-09-22-hack_x.htm.

[19] Tom W. Bell, "White-Hat Terrorism," *TechCentralStation*, November 7, 2003. http://www.techcentralstation.com/110703A.html.

[20] Michael Schrage, "We Can Trap More Crooks With a Net Full of Honey," Washington Post, January 11, 2004. p. B1. http://www.washingtonpost.com/ac2/wp-dyn/A5056-2004Jan9?language=printer.