A Site Where Hackers Are Welcome: Using Hack-In Contests To Shape Preferences and Deter Computer Crime

Brent Wible

INTRODUCTION

While the Internet has revolutionized communication and commerce, it has also created the conditions for a type of crime that can be committed anonymously, from anywhere in the world, and with consequences that are unprecedented in scope. With the failure of traditional law enforcement methods to deal with these challenges,[1] computer crime requires a new approach to thinking about deterrence. Focusing on a particular type of computer crime, unwarranted intrusions into private computer networks, this Note argues that "tailoring the punishment to fit the crime" might mean focusing on something besides punishment. It proposes a regulated system of privately sponsored "hack-in" contests to supplement the criminal law, which has proved inadequate at deterring computer crime.

Computer crime comes in many varieties, including online theft and fraud, vandalism, and politically motivated activities.[2] Other hackers simply try to break code, seeking challenge, competition, and bragging rights.[3]

1. *See infra* Part I (describing the difficulty of enforcing laws that criminalize hacking); *see also infra* text accompanying notes 120-124 (describing business losses due to computer crime).

2. The hack-in contest proposal is not designed to impact the behavior of these kinds of hackers. A hack-in contest is unlikely to provide a viable substitute for an antiglobalization activist who wants to vandalize a website or for a profit-motivated hacker who uses the computer as a tool to engage in old-fashioned crime. The contest proposal is especially suited to shaping the behavior of those hackers who enjoy challenge and seek bragging rights.

3. *See, e.g.*, Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 183-87 (2000) (recognizing three primary types of hacking: (1) politically motivated "hacktivism," (2) crime carried out by disgruntled employees, and (3) recreational hacking—including both malicious and nonmalicious activities—carried out for "the thrill of the challenge or for bragging rights in the hacking community" (citation omitted)); Peter Grabosky, Computer Crime: A Criminological Overview 3, *at* http://www.aic.gov.au/conferences/other/grabosky_peter/2000-04-vienna.pdf (last visited Nov. 25, 2002).

Whatever the motivation, intrusions have serious costs.[4] At the very least, a violated site must patch the security hole. Even a nonmalicious trespass disrupts the victim's online services while the breach is fixed. Not knowing whether or not a breach was malicious, companies generally expend resources investigating the matter, often hiring private investigators so that they do not suffer reputational loss.[5] If other hackers become aware of the site's vulnerability, a nonmalicious hack may be the precursor to more malicious attacks.[6] Finally, considering the gravity of the risk, attack victims may change their behavior, becoming reluctant to put valuable information online.[7]

How can private actors, alongside government, deter such activity? Two basic approaches have been suggested. First, some scholars have imagined creative ways of reinforcing the criminal law with other kinds of constraints on behavior.[8] Second, others have suggested that the least dangerous kinds of hacking should be decriminalized in ways that demarginalize the hacking community and actually increase Internet security.[9]

4. *See generally* Andrew Conry-Murray, *Strategies and Issues: Deciphering the Cost of a Computer Crime*, NETWORK MAG., Apr. 5, 2002, *at* http://www.networkmagazine.com/article/NMG20020401S0003 (discussing the kinds of costs that victims of computer crime bear and how to prove the amount of those costs in court). A 1995 survey by Ernst & Young found that of 1290 businesses, nearly half had suffered security breaches in the past two years, and at least twenty had incurred related losses exceeding one million dollars. *See* Joseph C. Panettieri, *Ernst & Young Security Survey: SECURITY*, INFORMATIONWEEK, Nov. 27, 1995, *at* http://www.informationweek.com/555/55mtsec.htm.

5. According to William J. Cook, author of the Justice Department's manual on computer prosecution, "organizations often swallow losses quietly rather than notifying the authorities and advertising their vulnerability to shareholders and clients." Marc S. Friedman & Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway*, 9 J. PROPRIETARY RTS. 2, 2 (1997) (citation omitted). Companies are increasingly pursuing private enforcement measures to monitor security breaches. In 2000, companies spent an estimated $300 billion on private enforcement. Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 100 (2001).

6. While companies are reticent to report security breaches and lose customers, they also fear that a reported hack both invites retributive attacks and highlights vulnerabilities to other hackers. *See* Pam Mendels, *Companies Found Sometimes Reluctant To Press Cybercrime Cases*, WASH. INTERNET DAILY, Apr. 24, 2002, at 4. The first hacker to gain access to a site may even engage in "war chalking," leaving marks identifying unprotected systems. Colin Barker, *We Have Nothing To Fear but Fear Itself*, COMPUTING, Sept. 27, 2002, at 39, *at* http://www.computing.co.uk/Features/1135465.

7. *See* D. Jean Veta et al., *Is Your Company Protected? Developing a Comprehensive Cyber-Security Plan To Mitigate Legal Exposure from Cyber-Crime*, CYBERSPACE LAW., July-Aug. 2002, at 5 (noting the potentially huge legal liability companies may face if their customers' proprietary information is stolen online).

8. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001).

9. *See, e.g.*, SUELETTE DREYFUS, UNDERGROUND: TALES OF HACKING, MADNESS AND OBSESSION ON THE ELECTRONIC FRONTIER 450-51 (1997), *available at* http://rubberhouse.sourceforge.net/underground/Underground.pdf; PAUL A. TAYLOR, HACKERS: CRIME IN THE DIGITAL SUBLIME (1999); Michael Lee et al., Comment, *Electronic Commerce,*

Those in the first group have expanded on the Beckerian framework, long dominant in thinking about deterrence, which limits policymakers to manipulation of two factors in deterring crime—probability of detection and severity of sentence.[10] Scholars looking beyond this framework have incorporated social norms,[11] architecture,[12] and monetary costs[13] as additional constraints on crime. Neal Katyal, for example, argues that monetary costs should supplement criminal sanctions because they constrain all actors, whereas legal sanction is only probabilistic.[14] The insight is well taken. Criminal constraints alone will not effectively deter computer crime. Law must help second and third parties—victims of computer crime and Internet users—deter crime themselves.[15]

Even this most recent scholarship at the vanguard of deterrence theory, however, approaches deterrence from a *cost* perspective. Departing from this tradition, this Note argues that, just as the "law should strive to channel crime into outlets that are more costly,"[16] it should also encourage mechanisms that channel criminal behavior into *legal* outlets.

The second group of scholars argues that "look-and-see" hacking, where hackers only explore systems without damaging them, and perhaps report that they have breached security, is victimless and should be decriminalized. They argue that decriminalization would result in a number of social benefits, including an increase in Internet security as hackers identify latent vulnerabilities, a better allocation of law enforcement resources, and the development of creative people with technological skills.[17] The arguments do not satisfy opponents of decriminalization,

Hackers, and the Search for Legitimacy: A Regulatory Proposal, 14 BERKELEY TECH. L.J. 839 (1999).

10. Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968).

11. Dan M. Kahan, *Social Influence, Social Meaning, and Deterrence*, 83 VA. L. REV. 349 (1997).

12. *See generally* LESSIG, *supra* note 8 (arguing that code, the architecture of the Internet, provides many constraints on web behavior); Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039 (2002) (showing how architecture—the construction of space—constrains behavior and can deter crime).

13. Katyal, *supra* note 8.

14. *Id*. at 1010.

15. *Id*. at 1013.

16. *Id*. at 1006.

17. *See, e.g.*, DREYFUS, *supra* note 9, at 452, 454 (arguing that punishing "look-and-see" hackers results in a misallocation of law enforcement resources); TAYLOR, *supra* note 9, at 43 (arguing that hacking "has been responsible for many of the most progressive developments in software development" (quoting ANDREW ROSS, STRANGE WEATHER: CULTURE, SCIENCE AND TECHNOLOGY IN THE AGE OF LIMITS 81 (1991)); Lee et al., *supra* note 9, at 882-86 (arguing that limited decriminalization may increase online security; reconstruct trust among hackers, law enforcement, and the computer security industry; and make the construction of cyberspace architecture less opaque); Douglas Hayward, *Hackers: Friends or Foes?*, TECHWEB, Sept. 15, 1997, *at* http://content.techweb.com/wire/news/1997/09/0915hackers1.html (quoting Paul Taylor as suggesting that by criminalizing all forms of hacking, society will lose many of the benefits derived from technological curiosity and creativity).

however, who emphasize that decriminalization fails to signal clearly that hacking is a proscribed activity.[18]

This Note seeks to develop a proposal—the "hack-in contest"—that appeals to both proponents and opponents of decriminalization. First, contests can capture the benefits of decriminalization without sacrificing the expressive and preference-shaping functions of the criminal law. Second, contests provide positive incentives for law-abiding hacking, an important approach given a hacking subculture that may be unreceptive to sanctions.[19] Seeking to introduce positive reinforcement and "channeling structures" into the toolbox of criminal deterrence,[20] this Note argues that a system of structured hack-in days will channel behavior away from illegal hacking toward approved activities. An effective system of contests may even strengthen positive norms among hackers, shaping preferences for law-abiding behavior.[21] While privately sponsored hack-in contests are already prevalent,[22] these contests lack regularity and fail to distinguish between approved and illegal hacking. Unlike these private contests, a regulated system of competitions should be designed to deter computer crime.

Part I of this Note outlines the current responses and proposals concerning computer crime and their general failure to prevent unwarranted intrusions. It contends that raising costs may not effectively deter hacking and that decriminalization undermines the expressive function of the criminal law. Part II begins by examining the preference-shaping function of the criminal law, arguing that "positive reinforcement" may be as effective at preference shaping as criminal sanctions. It then argues that the social norms latent in hacker culture may be more effectively harnessed by positive incentives than by sanctions. Part III proposes a hack-in contest framework that encourages law-abiding norms and shapes preferences for legal hacking. Part IV compares the contest proposal to broader decriminalization models and anticipates several objections to the proposal.

18. *See, e.g.*, Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 206 (2000).

19. *See, e.g.*, Naftali Bendavid, *FBI Hacks into Web of Intruders: Computer Rebels Hit Back with Daring Cyber-Pranks*, CHI. TRIB., May 29, 1999, § 1, at 1 (describing hacker taunts of the FBI and disrespect of law enforcement officials).

20. Positive reinforcement has been largely ignored both as a deterrent to crime and as a tool of rehabilitation, despite evidence indicating that the promise of reward may motivate actors even more than the threat of punishment. *See, e.g.*, Irving Piliavin et al., *Crime, Deterrence, and Rational Choice*, 51 AM. SOC. REV. 101, 117 (1986).

21. For an extended discussion of preference shaping, see Kenneth G. Dau-Schmidt, *An Economic Analysis of the Criminal Law as a Preference-Shaping Policy*, 1990 DUKE L.J. 1, 2 (arguing that, "in addition to creating disincentives for criminal activity, criminal punishment is intended to promote various social norms of individual behavior by shaping the preferences of criminals and the population at large").

22. *See infra* Section III.A (describing the prevalence, structure, and goals of private hack-in contests).

I. PREVIOUS RESPONSES AND PROPOSALS CONCERNING COMPUTER CRIME

A. *Law, Code, and the Market*

The first cases of computer crime were heralded as an unprecedented phenomenon that law was not equipped to handle.[23] Scholars and policymakers have since proposed a number of deterrence strategies, from criminal sanctions to tort law and the architecture of the web itself, but none of these methods has proved successful at deterring criminal hacking.

Congress prohibited unwarranted intrusions in the Computer Fraud and Abuse Act of 1984 (CFAA).[24] Among other problems, prosecutorial difficulties have minimized the CFAA's deterrent effect. Shortly after criminalization, the low number of prosecutions prompted some to suggest that antihacking laws were largely symbolic.[25] Enforcement remains difficult, especially given the near impossibility of prosecuting attempts under 18 U.S.C. § 1030(b),[26] and the need for a great investment of time, resources, and skill—even assuming that local law enforcement agents have the requisite training.[27] Digital anonymity, encryption technologies, and the circuitous process of electronic tracing give cybercriminals an advantage over law enforcement.[28] With jurisdictional uncertainties looming in cases that are expensive to investigate and that require sophisticated tracking capabilities, state prosecution is almost impossible.[29]

23. *See, e.g.*, Christopher D. Chen, Note, *Computer Crime and the Computer Fraud and Abuse Act of 1986*, 10 COMPUTER/L.J. 71, 84 (1990) (arguing that education about computer abuse is necessary given that law is insufficient to solve computer crime); Brenda Nelson, Note, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER/L.J. 299, 299 (1991) (describing, in the precriminalization days, the struggle to apply traditional criminal law doctrines to computer abuse).

24. 18 U.S.C. § 1030 (2000).

25. *See* Michael P. Dierks, *Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 328 (1993) (noting that during the first six years of the CFAA, the only successful prosecution was that of Robert Morris); *see also* Kenneth Rosenblatt, *Deterring Computer Crime*, TECH. REV., Feb.-Mar. 1990, at 35.

26. First, the CFAA requires that hackers cause reckless or negligent damage before they may be prosecuted. 18 U.S.C. § 1030(a)(5)(A)(ii)-(iii). This is much less likely to occur during an attempt than during an actual intrusion. *See* Calkins, *supra* note 18, at 196-97. Second, the significant difficulties targets face in detecting successful intrusions are exaggerated with mere attempts.

27. *Cybercrime: Hearing Before the Subcomm. on Commerce, Justice, and State, the Judiciary, and Related Agencies of the Senate Appropriations Comm.*, 106th Cong. 27-30 (2000) [hereinafter *Cybercrime Hearing*] (statement of Louis J. Freeh, Director, FBI) (noting the lack of training at the state level).

28. *See* Katyal, *supra* note 8, at 1047-48.

29. Friedman & Bissinger, *supra* note 5, at 10 ("Most states do not have divisions of their police force or district attorney staff dedicated to cases of computer theft, damage or injury and what is often perceived as victimless crime gets shuffled to the side."); Rustad, *supra* note 5, at 98-99; U.S. DEP'T OF JUSTICE, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET 34 (2000), *at* http://www.usdoj.gov/

Proponents of tort liability for computer crime argue that, as compared to the criminal law, civil actions give targets control over the litigation.[30] The possibility of obtaining damages gives targets, otherwise unwilling to admit electronic vulnerabilities to consumers, an incentive to report.[31] While Internet Service Provider (ISP) liability has received the most attention as a serious proposal,[32] four varieties of tort liability are possible in the computer-crime context—(1) hacker liability, (2) ISP liability, (3) security company liability, and (4) liability for victims who fail to take private precautions. A general but significant critique of these proposals is that tort liability does not carry a strong symbolic message condemning illegal hacking. The various tort proposals are unlikely to succeed for specific reasons, too: hackers tend to be judgment proof,[33] holding ISPs liable may actually increase hacking,[34] holding security companies to a high standard of liability may make their products prohibitively expensive and may be less effective than providing incentives to good practice,[35] and

criminal/cybercrime/unlawful.htm (citing the barriers to state enforcement, such as lack of resources, jurisdiction, subpoena power, etc.).

30. *See* Ian C. Ballon, *Alternative Corporate Responses to Internet Data Theft*, *in* 17TH ANNUAL INSTITUTE ON COMPUTER LAW 737, 744 (PLI Patents, Copyrights, Trademarks & Literary Prop. Course, Handbook Series No. 471, 1997) (describing the benefits of civil, as opposed to criminal, computer-crime actions).

31. *See* David L. Gripman, *The Doors Are Locked but the Thieves and Vandals Are Still Getting in: A Proposal in Tort To Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 174-76 (1997); Daniel Sieberg, *FBI: Cybercrime Rising, yet Fewer Companies Reporting Incidents*, CNN.COM, Apr. 8, 2002, *at* http://www.cnn.com/2002/TECH/internet/04/07/cybercrime.survey/index.htm ("Many firms cite the fear of bad publicity for their reluctance to alert authorities, while others prefer not to divulge any proprietary information to investigators.").

32. *See, e.g.*, Katyal, *supra* note 8, at 1095-101 (discussing difficulties with ISP liability). *See generally* TIMOTHY D. CASEY, ISP LIABILITY SURVIVAL GUIDE: STRATEGIES FOR MANAGING COPYRIGHT, SPAM, CACHE, AND PRIVACY REGULATIONS (2000) (showing ISPs how to protect themselves and limit their liability as governments around the world establish laws and regulations relating to the Internet).

33. *See* Ian C. Ballon, *The Law of the Internet: Developing a Framework for Making New Law*, *in* FIRST ANNUAL INTERNET LAW INSTITUTE 9, 15 (PLI Patents, Copyrights, Trademarks & Literary Prop. Course, Handbook Series No. 482, 1997) ("Internet tortfeasors and infringers are likely to include a high percentage of students and others who may not have the resources to satisfy large judgments.").

34. Hackers, aware that targets are likely to focus their legal efforts on the party with deep pockets, have an incentive to launch their attacks from such deep-pocket ISPs. Moreover, because ISPs gain little from risky subscribers, saddling ISPs with liability for the acts of their subscribers may lead to the expulsion of a number of users, threatening the Internet's potential benefits. Calkins, *supra* note 18, at 215-16, 219.

35. Some efforts to encourage good security practice are already underway. *See* Charles Babington, *Clinton Plan Targets "Cyber-Terrorism*,*"* WASH. POST, Jan. 8, 2000, at E1 (describing college scholarships for students planning to enter the computer security field in exchange for their public service after graduation); Vernon Loeb, *Launching a Counteroffensive in Cyberspace: Program Training Corp of Experts in Computer Security*, WASH. POST, Feb. 5, 2000, at A3 (describing government efforts to train experts); Dan Verton, *Schmidt Lays Out Cyberprotection Board Agenda*, CNN.COM, Mar. 15, 2002, *at* http://www.cnn.com/2002/TECH/industry/03/15/cyberprotection.agenda.idg/index.html (describing the federal government's efforts to coordinate a national approach to protect essential networks).

making victims bear the cost evinces an overly optimistic faith in the ability of potential targets to safeguard their materials through technological solutions.[36]

Just as tort law fails to provide a practical response to computer crime, reliance on market solutions would lead many firms to take extreme measures to protect themselves from vulnerability, potentially resulting in undesirable architectural rules.[37] Alternatively, one may discern a "broken windows" effect if companies rely too heavily on self-help.[38] While visible self-help measures like protective software are essential and instill confidence in the technological infrastructure, paradoxically, they may lead to more crime.[39] Hackers may interpret the flowering of private security measures as an indication of profligate hacking or lackluster monitoring and as an invitation to hack.[40]

Security software is not the only technology that could be used to deter hacking. Lawrence Lessig has been the most original and vocal proponent of the idea that while behavioral constraints are modified by changing law in real space, in cyberspace, constraints are more effectively altered by changing code.[41] While his approach is meta-architectural and does not focus on individual security measures like security software, code is inadequate to constrain hackers. Dorothy and Peter Denning have argued that "the solutions . . . cannot be achieved solely by technological means.

36. Faith in technological solutions is especially inappropriate given the prevalence of "social engineering"—inducing authorized persons to reveal passwords. *See* Jonathan J. Rusch, *Don't Look Now*, 9 GEO. MASON L. REV. 289, 298 (2000).

37. *See* LESSIG, *supra* note 8, at 59-60, 83, 98-99 (arguing that code embodies values congruent with the interests of Internet commerce and that relatively invisible regulations, such as regulation through code, lack transparency and are difficult to resist, resulting in undesirable rules).

38. *See generally* James Q. Wilson & George L. Kelling, *Broken Windows*, ATLANTIC MONTHLY, Mar. 1982, at 29 (arguing that the appearance that crime is rampant encourages more crime and that by reducing the visibility of social disorder, serious crime can be deterred).

39. *See Network Security: Easy To Use but Hard To Get Right*, COMPUTING, Mar. 28, 2002, at 39 (suggesting that off-the-shelf security software can be more dangerous than having no protection at all by creating a false sense of security and leading to unsafe practices that are visible to hackers); Tony Dreier, *To Protect and To Surf*, PC MAG., Feb. 26, 2002, *at* http://www.pcmag.com/print_article/0,3048,a=21990,00.asp (noting that many firewalls promising zero maintenance lull users into a false sense of security, fail to alert them to new hacking techniques, and indicate optimal targets to hackers).

40. Like in real space, security measures result from a fear of crime. Private measures indicate a failure of criminal law to deter cybercrime, and these measures have not proven effective at deterring crime themselves. *See Hackers Never, Ever Stop Hacking*, INFOTECH WKLY., Sept. 3, 2001, at 20 (noting that security measures are reactive and that the security industry is driven forward by a need to patch security vulnerabilities); *cf.* Kahan, *supra* note 11, at 389 ("[W]hen they feel reassured that law enforcement is adequate, law-abiders are *more* likely to view private precautions as worthwhile, and less likely to see such precautions as signs that those around them lack confidence in the efficacy of law."); Katyal, *supra* note 8, at 1109-11 (drawing on the "broken windows" theory and arguing that visible signs of disorder in cyberspace breed further disorder).

41. Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMMLAW CONSPECTUS 181, 184 (1997).

The answers will involve a complex interplay among law, policy, and technology."[42] Moreover, many hackers turn to "social engineering," not technology, when looking for weaknesses in computer networks.[43] Hackers often manipulate authorized users to gain access to networks, a practice that is impossible to stop with technological solutions.[44] Because sophisticated hackers are not susceptible to regulation through code, code must be supplemented to deter computer crime. Even in Lessig's own terms, code must be complementary to the other "modalit[ies] of regulation"—law, social norms, and the market.[45] Yet it is precisely these mechanisms that have proved unable to constrain illegal hacking effectively.

Unsatisfied with these approaches to computer crime, Katyal has argued that raising perpetration costs, incurred by all who commit crime, may be more effective.[46] While the insight is provocative, some of his proposals remain impractical. Charging fees to enter sites, while making hacking more costly, may pose barriers to Internet commerce that overly restrict productive uses. Likewise, it is not immediately evident how a market for hacker tools could be constructed, since they are easy to post on the web. Given foreign markets and jurisdictions, it may be impossible to impose prices on these tools.[47]

B. *Decriminalization Proposals and Their Difficulties*

Decriminalization is often suggested for "victimless crimes"—legally prohibited activities that involve no unwilling or complaining party.[48] Drug use and prostitution are prominent examples. Among computer crimes, nonmalicious intrusions, often characterized as "look-and-see" hacking, are the strongest candidate.[49] Not surprisingly, some argue that this kind of hacking should be decriminalized or regulated by a "duty to report."[50]

Proponents of decriminalization make five essential claims about its benefits. First, decriminalization would lead to increased Internet security

42. Dorothy E. Denning & Peter J. Denning, *Preface* to INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS, at vii, x (Dorothy E. Denning & Peter J. Denning eds., 1997).

43. David B. Fein & Mark W. Heaphy, *Options when a System Has Been Hacked: Fear of Bad Publicity Elicits Corporate Fight or Flight*, CONN. L. TRIB., Dec. 17, 2001, at 2.

44. *Id*.

45. LESSIG, *supra* note 8, at 87-90.

46. Katyal, *supra* note 8, at 1010.

47. *See* Ellen S. Podgor, *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. DAVIS L. REV. 267, 281-84 (2002) (discussing the complexities involved in determining jurisdiction over computer crime internationally).

48. *See, e.g.*, Kent Roach, *Four Models of the Criminal Process*, 89 J. CRIM. L. & CRIMINOLOGY 671, 680 (1999).

49. As suggested in the Introduction and *infra* text accompanying notes 172-174, nonmalicious hacking is hardly victimless.

50. Lee et al., *supra* note 9, at 882-83.

as hackers identify latent security flaws.[51] Second, as hackers made security tighter, a reconstruction of trust among hackers, law enforcement personnel, and security professionals would follow.[52] Third, by decriminalizing the most minimally harmful hacking, law enforcement resources would be conserved and concentrated on more destructive hacking.[53] Fourth, under a blanket prohibition on hacking, we lose the social benefits of creating a space where technological skills can be developed in creative ways.[54] Fifth, limited decriminalization may help bridge the cultural gap between hackers and regular Internet users, opening up a discussion of the policy implications of changes in code. Under the presence of hackers' watchful eyes, the implementation of architectural changes in cyberspace is more likely to reflect democratic principles.[55]

The most prominent and narrowly circumscribed decriminalization proposal in the legal literature to date is the "duty to report." Proponents of this reporting duty defend it by arguing that "[s]uccessful incidents of unauthorized access should be presumed by law to be nonmalicious if the actor makes a good-faith effort to report the incident to the proprietor of the accessed system immediately upon obtaining access."[56] The implication is that a reported hack could not have been malicious and that the "target" site is not a victim. These authors claim that the rule would (1) lead to cooperation and mutual trust between hackers and law enforcement; (2) revive self-regulating, law-abiding norms among hackers; and (3) increase Internet security.[57]

Even modest decriminalization plans like the duty to report seek these benefits at the cost of undermining the criminal law.[58] The reporting rule, which presumes that any episode of reported unauthorized access is nonmalicious, does not absolutely prohibit any behavior and is unlikely to deter computer crime. Since it does not attach a value judgment to unauthorized access per se, the rule could not shape preferences.

51. *Id*. at 883.

52. *Id*. at 883-84.

53. DREYFUS, *supra* note 9, at 452-54 ("[A] great deal of time and money has been wasted in the pursuit of look-see hackers. . . . Make look-see hacking a minor offence and the institutions will stop going after the soft targets and hopefully spend more time on the real criminals.").

54. TAYLOR, *supra* note 9, at 51 (finding that hacking is "curiosity-driven" and motivated by "relentless pursuit of the answer to a technical problem").

55. Lee et al., *supra* note 9, at 885-86 (arguing that as decriminalization bridges the cultural gap between hackers and ordinary Internet users, hackers could become "a loosely organized coalition of consumer advocates who could provide a forum, however informal, for the discussion and implementation of code at a collective level" and that hackers could provide ordinary users important information about the consequences of architectural developments).

56. *Id*. at 882-83.

57. *Id*. at 883-85.

58. *See* Calkins, *supra* note 18, at 203-09 (arguing that the reporting rule will neither deter computer crime nor shape hacker preferences); *infra* Section IV.A.

II. PREFERENCE SHAPING, HACKER CULTURE, AND SOCIAL MEANING

The criminal law does not simply inspire rational calculations about the probability of detection and the severity of the punishment.[59] Kenneth Dau-Schmidt famously analyzed the criminal law as a *preference*-shaping policy, suggesting that criminal laws seek to influence tastes or preferences as much as to constrain opportunity.[60] While some have argued that even limited decriminalization of computer crime makes preference shaping inefficient or impossible,[61] this Part argues that preference shaping would actually be *enhanced* by a limited, "safe harbor" decriminalization within clear boundaries.

Since hacker culture has many antiauthoritarian strands, preference shaping on a punishment model alone is unlikely to succeed. On its own, the criminal law may strengthen the contours of a criminally deviant subculture. Thus, positive incentives for lawful conduct, a necessary component of decriminalization, must play an essential role in preference shaping in order to reinforce the positive and law-abiding social meanings latent in hacker culture.[62] By drawing on the positive aspects of the "hacker ethic," positive incentives can help develop socially beneficial preferences within hacker communities.

A. *Preference Shaping with Positive Incentives*

The preference-shaping model requires that the regulator first identify the preferred social mores before setting penalties and incentives to shape preferences. Because the cost of preference shaping is so high, Dau-Schmidt argues, it should only be used when society values one activity highly and the other only minimally.[63] If preference shaping is to work, the undesirable activity must be clearly prohibited. Hacking is clearly prohibited by the criminal law. One might argue that even minimal decriminalization would upset the clarity of the rules, making preference shaping inefficient.

59. Gary Becker pioneered modern economic analysis of criminal deterrence, focusing on whether a particular penalty and the enforcement of that penalty would deter commission of the crime. *See generally* Becker, *supra* note 10.

60. Dau-Schmidt, *supra* note 21.

61. Calkins, *supra* note 18, at 203-09.

62. *See* Kahan, *supra* note 11, at 365-66, 380-83. Kahan argues that criminal law helps shape social meaning and that criminal deterrence strategies based on high sanctions and a low probability of capture reduce levels of cooperation with law enforcement. With computer crime, where the applicable sanctions are relatively high and the probability of capture is low, a nonpenal deterrence strategy may prove more fruitful than a strict punishment regime.

63. Dau-Schmidt, *supra* note 21, at 19-22.

Decriminalization within clear boundaries, however, would not upset the preference-shaping policy of the criminal law. Rather, to the extent that the decriminalization program provides incentives for socially approved behavior, it would enhance that preference-shaping function. Dau-Schmidt recognizes the role that reward plays in shaping preferences.[64] While his primary concern is to understand the function of the criminal law, he emphasizes various preference-shaping technologies, including positive incentives.[65] Thus, preference shaping that is begun through criminalization can be reaffirmed through positive reinforcement.

Dau-Schmidt is not alone in recognizing the deterrent and preference-shaping power of positive incentives. Philosophy has not missed the point.[66] Philosophers have recognized reward, like punishment, as an ex ante deterrent to criminal behavior that encourages good conduct.[67] Empirical research confirms this intuition. Social scientists have argued that threat of punishment does not act as a strong deterrent for people who are criminally motivated or morally uncommitted.[68] A more determinative factor is the scale of the opportunity to earn rewards from criminal activities.[69] The argument seems applicable to the computer-crime context, where, in the absence of a sociomoral consensus on hacking, many actors remain morally uncommitted.[70] In the hacker world, the threat of punishment may be overshadowed by the expectation of psychic rewards—including intellectual stimulation, the thrill of competition, and gains to self-esteem

64. *Id*. at 5.

65. *Id*. at 18 (describing the use of rewards and education to shape preferences and views about particular behaviors); *see also id*. at 17 n.80 (listing a number of nonpunitive methods of preference shaping).

66. Donald Clark Hodges, *Reward*, 19 PHIL. & PHENOMENOLOGICAL RES. 198, 202-03 (1958) (noting that positive incentives can be used to encourage good conduct and enhance social welfare).

67. *See* JEREMY BENTHAM, THE LIMITS OF JURISPRUDENCE DEFINED 224-25 (Charles Warren Everett ed., 1945) ("This punishment then, or this reward, whichever it may be, in order to produce its effect must in some manner or other be announced: notice of it must in some way or other be given, in order to produce an expectation of it, on the part of the people whose conduct it is meant to influence."); DAVID HUME, *An Enquiry Concerning the Principles of Morals*, *in* HUME'S MORAL AND POLITICAL PHILOSOPHY 173, 194 (Henry D. Aiken ed., 1948) (arguing that, in order to give incentives for production and accomplishment, "whatever is produced or improved by a man's art or industry ought . . . to be secured to him"). Hume thus implicitly regards reward less as a *recognition of* virtuous action than as a *stimulus to* such conduct.

68. Piliavin et al., *supra* note 20.

69. *Id*. at 114; *cf*. W. Kip Viscusi, *The Risks and Rewards of Criminal Activity: A Comprehensive Test of Criminal Deterrence*, 4 J. LAB. ECON. 317, 338-39 (1986) (noting the impact of the potential financial rewards of criminal activity on decisionmaking).

70. *See* Mark D. Rasch, *Criminal Law and the Internet*, *in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES 141, 145, 164 (Joseph F. Ruh, Jr., ed., 1996) (arguing that, for example, the problem of property in cyberspace admits of no easy legal or moral answers, suggesting that "moral and legal structures break down in cyberspace," and implying that no social consensus has yet emerged to categorize many activities on the web).

and reputation derived from success.[71] If this is the case, a preference-shaping model grounded in positive incentives makes sense.

To the extent that criminal sanctions for computer crime are meant to shape preferences by *teaching* specific behaviors, rewards may better achieve that goal. Psychology posits that positive reinforcement results in more effective learning than punishment. Whereas punishment often leads the punished actor to feel subservient, rewards encourage feelings of independence and may thus result in higher rates of rule compliance.[72] By appealing to hackers' sense of independence, a recognition that some kinds of hacking are legitimate may thus shape preferences for these activities.

Finally, the psychology of human choice reinforces the importance of positive incentives in decisionmaking processes. An influential psychological study found that in choosing among options, we simultaneously choose an option for its positive characteristics while rejecting others for their negative qualities.[73] Criminal law encourages us to reject crime by emphasizing its negative consequences. But a consideration of the negative only constitutes half of a decisionmaking process. By framing a choice as one between an activity with negative consequences and one with positive attributes, a balanced policy may more effectively deter computer crime than does threat of criminal sanction alone.[74] A particular characteristic of hacker culture—its status as a subculture relatively resistant to criminal sanctions—reinforces the need to add positive incentives to the preference-shaping model in the computer-crime context.

71. *See* Grabosky, *supra* note 3, at 3 ("The very fact that some activities in cyberspace are likely to elicit official condemnation is sufficient to attract the defiant, the rebellious, or the irresistibly curious.").

72. *See generally* Robert Eisenberger & Linda Rhoades, *Incremental Effects of Reward on Creativity*, 81 J. PERSONALITY & SOC. PSYCHOL. 728 (2001) (arguing that external rewards can enhance perceived self-determination, increase task interest, and create positive relationships). *Cf.* BRUNO FREY, NOT JUST FOR THE MONEY: AN ECONOMIC THEORY OF PERSONAL MOTIVATION 18 (1997) (arguing that if an intervention acknowledges an actor's intrinsic motivation, the intervention will be perceived as supportive).

73. Edlar Shafir et al., *Reason-Based Choice*, 49 COGNITION 11, 15 (1993).

74. Once some kinds of hacking become acknowledged as socially legitimate, random unauthorized access is likely to be considered as a more extreme activity than participating in contests. Extremeness aversion predicts that within an offered set, options with extreme values are relatively less attractive than those with intermediate values. Itamar Simonson & Amos Tversky, *Choice in Context: Tradeoff Contrast and Extremeness Aversion*, 29 J. MARKETING RES. 281, 289-92 (1992) (describing the phenomenon of "extremeness aversion," whereby decisionmakers choose the "moderate" option); Cass R. Sunstein, *Behavioral Analysis of Law*, 64 U. CHI. L. REV. 1175, 1181-82 (1997) (finding that framing a choice between a moderate and an extreme option leads most actors to select the moderate course).

B. *Social Meaning in Hacker Culture*

Legal responses to crime may be ineffective or worse if they do not account for the social context in which they are applied and are not careful about the social meaning that a particular penalty may convey in that context.[75] Penalties for computer crime may thus have minimal effect to the extent that hackers constitute a counterculture. Penalties might serve less as a deterrent than as a challenge, something to boast about eluding.[76] Thus, punishment alone may not be the best preference-shaping model in the computer-crime context.

Sociologists have emphasized the adverse consequences of social reactions generated by deviance.[77] Labeling, the process of social sanctioning along the lines of group identity, may alter identities in ways that systematize and prolong deviance.[78] Deviance labeling produces changes in the actor's self-evaluation in which a deviant person reorganizes the self around deviant values, identities, and activities.[79] Broad criminalization of hacking under the CFAA is much like labeling. Sanctioning a broad category of conduct as criminal, especially when an identifiable social group primarily engages in that conduct, may lead to further deviance.[80] The Act's broad purview may help establish an antiauthoritarian subcommunity, a cohesive group defined by its commitment to "deviant" values. Standing alone, the criminal law may undermine efforts to deter computer crime. To strengthen preference shaping, positive reinforcement that draws on, rather than antagonizes, hacker culture may be more appropriate and may enhance the preference-shaping function of the criminal law.

We have remarked that, in order to effectively reduce crime, policies must support the positive social norms that already exist within the

75. Kahan, *supra* note 11, at 378; Neal Kumar Katyal, *Deterrence's Difficulty*, 95 MICH. L. REV. 2385, 2445 (1997) ("When the law is out of step with the norms in a given community, and it labels 'ordinary' citizens lawbreakers, the ability of the law to shape the behavior of that community is compromised. The individual lawbreaker—whose reputation may even have been enhanced by the skirmish with the police—is not as likely to heed a law-following message as a resident of a community where the law tracks its norms.").

76. *See* Bendavid, *supra* note 19; Marc Rogers, A New Hacker Taxonomy 12, *at* http://psyber.letifer.org/downloads/priv/hacker_doc.pdf (last visited Mar. 4, 2003) ("Psychological theories of crime postulate that because a hacker sub-culture or sub-class exists, and the activity is being reinforced . . . , criminal hacking will not disappear on its own but will continue to flourish if left unchecked." (citation omitted)).

77. *See generally* EDWIN M. LEMERT, SOCIAL PATHOLOGY: A SYSTEMATIC APPROACH TO THE THEORY OF SOCIOPATHIC BEHAVIOR (1951) (exploring the relationship between deviant activities and the organized social responses that identify, label, and control such deviance).

78. *See, e.g.*, L. Edward Wells, *Theories of Deviance and the Self-Concept*, 41 SOC. PSYCHOL. 189, 192 (1978).

79. *Id*. at 193, 200.

80. Charles R. Tittle, *Deterrents or Labeling?*, 53 SOC. FORCES 399, 408 (1975).

specified community.[81] Such norms exist in hacker culture, though their strength has waned. The Internet has diluted norms that were strong in the original, homogenous, tightly knit hacker community. Hackers were generally united by a code of ethics and a drive to understand technology.[82] They held themselves to high standards of behavior and scorned those who hacked maliciously.[83]

This early "hacker ethic" included principles such as "access to computers should be unlimited and total,"[84] "[a]ll information should be free,"[85] and "do not intentionally damage *any* system."[86] Hackers did not consider unauthorized access without malicious intent to be unethical.[87] In fact, many hackers believed hacking to serve a useful purpose by uncovering security flaws and vulnerabilities.[88]

81. Kahan, *supra* note 11, at 383-84 (arguing that "[t]he meaning a punishment expresses counts as much as the disutility it imposes"); Katyal, *supra* note 75, at 2445.

82. Dorothy E. Denning, Concerning Hackers Who Break into Computer Systems 7-9 (Oct. 1, 1990), *at* http://www.cpsr.org/cpsr/privacy/crime/denning.hackers.html.

83. BILL LANDRETH, OUT OF THE INNER CIRCLE 19 (1985) ("We were explorers, not spies, and to us, damaging computer files was not only clumsy and inelegant—it was wrong."); Denning, *supra* note 82, at 7 ("Hackers say they are outraged when other hackers cause damage or use resources that would be missed, even if the results are unintentional and due to incompetence.").

84. STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 27 (1984). Levy described the emergence of a hacker code of ethics, listing its tenets:

(1) "Access to computers—and anything which might teach you something about the way the world works—should be unlimited and total."
(2) "All information should be free."
(3) "Mistrust Authority—Promote Decentralization."
(4) "Hackers should be judged by their hacking, not [by other] criteria . . . ."
(5) "You can create art and beauty on a computer."
(6) "Computers can change your life for the better."

Id. at 27-33; *see also* The Mentor, A Novice's Guide to Hacking—1989 Edition (Dec. 1988), *at* http://www.undergroundnews.com/files/texts/underground/hacking/guide.htm. "The Mentor," one of the members of the Legion of Doom hacking group, presents the following set of guidelines for beginning hackers:

I. Do not intentionally damage *any* system.
II. Do not alter any system files other than ones needed to ensure your escape from detection and your future access . . . .
III. Do not leave your (or anyone else's) real name, real handle, or real phone number on any system that you access illegally. . . .
IV. Be careful who you share information with. . . .
V. Do not leave your real phone number to anyone you don't know. . . .
VI. Do not hack government computers. . . .
VII. Don't use codes unless there is *no* way around it . . . .
VIII. Don't be afraid to be paranoid. . . .
IX. Watch what you post on boards. . . .
X. Don't be afraid to ask questions. . . .
XI. Finally, you have to actually hack. . . .

Id.

85. LEVY, *supra* note 84, at 27.

86. The Mentor, *supra* note 84.

87. *See* LEVY, *supra* note 84, at 27-28; Denning, *supra* note 82, at 7-8.

88. Some hackers view themselves as part of a consumer-advocacy group, discovering security flaws in commercial network software and publishing it online. While the strategy may

The Internet has radically altered the social conditions that nurtured this ethic. While today hackers are often depicted as isolated, nocturnal individuals, early hackers tended to bond together in groups through which their ethic was enforced. Before the Internet, private networks called bulletin board systems hosted most hacking organizations. Generally led by a hacker with power to accept or exclude others from the group, these organizations were able to enforce norms. With a hierarchy based on knowledge and expertise, the groups were headed by their most technically proficient member, who tended to have gone through the norm-reinforcing process.[89] Those who violated norms were often rejected from the organization.[90] Widespread Internet use upset this socialization process. Few web users now undergo any normative socialization, and hackers freely surf the web, often posting their techniques online.[91]

While a cohesive hacker community bound by ethical guidelines is no longer dominant, remnants of the old "hacker ethic" remain. For example, the hacking competitions sponsored by security firms promise large rewards, but the hackers who participate stress that their aim is to improve programming by exposing deficiencies in code.[92] Some hackers are helping law enforcement fight the war on terror out of a desire to put their skills to productive use.[93] Finally, contrary to the standard image that security professionals and hackers are enemies, the two camps come together for Black Hat, the annual security conference, and DEFCON, the hackers'

result in increased hacking in the short term, such hackers argue that if they simply reported the vulnerability to those responsible, the weakness would be swept under the rug. Bruce Gottlieb, *Hack, CounterHack*, N.Y. TIMES, Oct. 3, 1999, § 6 (Magazine), at 34, 36 (reporting that Senators Fred Thompson and Joseph Lieberman lauded one such group, L0pht, for performing an important public service); *see also* Ellen Messmer, *@Stake's Pitch: Hackers Are Your Friends*, NETWORK WORLD, Feb. 7, 2000, *at* http://www.nwfusion.com/news/2000/0207apps.html (describing the security start-up @Stake, founded by Mudge, which employs hackers to test corporate networks for vulnerabilities).

89. Lee et al., *supra* note 9, at 867.

90. *Id*. The social norms literature indicates that small communities, where individuals are known, their activities are visible, and reputational sanctions are frequent, are the most likely venue for norms to have effect. *See* ROBERT C. ELLICKSON, ORDER WITHOUT LAW 167 (1991) (arguing that "members of a close-knit group develop and maintain norms whose content serves to maximize the aggregate welfare that members obtain in their workaday affairs with one another"); Elizabeth S. Scott, *Social Norms and the Legal Regulation of Marriage*, 86 VA. L. REV. 1901, 1922 (2000) ("Small communities are effective norm enforcers . . . because community members all know one another and interact on an ongoing basis. . . . Moreover, sanctions are particularly effective because in a small community, the potential norm violator is likely to value highly the esteem of community members.").

91. Hacking techniques are disseminated through many high school and university computer groups. Hacking magazines, like *www.2600.com*; hacking books, like *www.happyhacker.org/hhbook/toc.shtml*; hacking websites, like www.phrack.org, www.l0pht.com, and www.zerberus.de/texte/ccc/ccc95/artikel/hackan_e.htm; and hacking search engines, like www.astalavista.box.sk, are a source of much information.

92. *See infra* Section III.A.

93. *Cyber Security: Hacking for a Higher Power?*, NAT'L JOURNAL'S TECH. DAILY, Oct. 18, 2001, *at* http://nationaljournal.com/members/search.

shadow convention, annually separated only by a few days and a few blocks. The conventions draw essentially the same crowd,[94] and reports note the hacker desire to build confidence in the high-tech infrastructure by making code more secure.[95] Something remains of the original ethical principles.

Can these principles regain their normative force in the Internet age? While Lessig believes that amorphous identities and the lack of physical presence make regulation through social norms difficult in cyberspace,[96] Katyal argues that law can entrench social norms by placing computers in observable places and educating children about proper web behavior.[97] While real-space policies could encourage positive social norms, we should not forswear regulation through social norms via the Internet itself. The confluence of contests, codes of ethics, and publicity campaigns, along with real-space strategies, could cultivate positive social norms in cyberspace.[98]

The roots of the original hacker ethic are still present. Policies meant to deter computer crime should be cognizant of these latent values. The use of criminal punishment alone may contribute to their demise. The *interaction* of positive incentives and punishments could revitalize and strengthen these traditional norms, filling in gaps that the Internet has created.[99] An effort must be made to help rebuild a community of hackers in which a body of positive social norms can be sustained. Contests can contribute to the norm-rejuvenating process. After all, group interactions play an important role in shaping normative definitions of acceptable behavior.[100]

III. CONTESTS AND THE NEW HACKER

Although contests are an integral part of hacker culture, they have untapped potential as a policy tool. This Part begins by describing how hacker contests are currently used. It concludes by laying out a rough contest framework that could deter computer crime. While law must continue to impose sanctions upon cybercrime, private ordering can help minimize the problem. The contest model responds to the insights of

94. Matthew Fordahl, *Schmoozing with the Web Enemy*, CHI. TRIB., Jul. 16, 2001, § 4, at 5.

95. *Id*.

96. LESSIG, *supra* note 8, at 14-17.

97. Katyal, *supra* note 8, at 1108-09; *cf. Cybercrime Hearing*, *supra* note 27, at 22-23 (statement of Louis J. Freeh, Director, FBI) (arguing that schools and workplaces must become more conversant in an ethical discourse about computer use).

98. Pseudonymity for tournament participants may also contribute to the development of positive hacker social norms. Insofar as pseudonyms allow for the accumulation of reputational capital, they may help create social norms in the hacking tournaments that have spillover effects beyond the contest context. *See infra* notes 162-166 and accompanying text.

99. *See infra* Section III.B.

100. Ronald L. Akers et al., *Social Learning and Deviant Behavior: A Specific Test of a General Theory*, 44 AM. SOC. REV. 636, 638 (1979).

preference-shaping theory, maintaining a clear prohibition on illegal activities while providing incentives for socially approved hacking. Privately sponsored contests can complement law both to deter computer crime and to reap the benefits of legitimately victimless hacking.

A. *The Prevalence of Hacker Competitions*

Hacker competitions are common. At hacker conventions, attendees frequently attempt to hack into each other's systems while protecting their own.[101] The security industry sponsors contests to perfect products, challenging industry professionals to hack into servers.[102] Most interesting is the strategy that some security companies have taken in recent years. As a means of advertising their products and endorsing them with a rigorous public test, they have challenged hackers to crack their code.[103] Sponsoring a site secured by their software, the companies have promised rewards to the first hackers able to breach security.[104] The contests are popular among hackers. One contest last year logged almost 20,000 attacks.[105] The companies carefully tailor their competitions to the participants' motivations. They recognize the importance of "bragging rights" and promote the tournaments to appeal to hackers' competitive spirit. More than a passing fad, competitions are increasingly prevalent,[106] and some of them

101. Mathias Thurman, *Security Manager's Visit to Def Con Is an Eye-Opener*, COMPUTERWORLD, Aug. 13, 2001, ¶ 3, *at* http://www.computerworld.com/securitytopics/security/story/0,10801,62960,00.html.

102. Jennifer L. Rich, *Brazilian Company Is Hacking Its Way up*, N.Y. TIMES, Feb. 26, 2001, at C5 (describing the annual security industry hacking contest sponsored by the Sans Institute).

103. That a company can withstand hacker attacks is an effective endorsement. The website of one security company, AntiOnline, is continuously targeted by hackers. AntiOnline, *at* http://www.antionline.com/index.php (last visited Feb. 15, 2003). Its founder, John Vranesevich, established the site as one that trumpeted hacker exploits, but that has changed since Vranesevich started to pursue hackers as a security expert. That his site withstands the attacks is its biggest selling point. Vranesevich has capitalized on the situation, including a feature visitors can use to see who is trying to hack in at any particular moment. Mark Compton, *Cybersleuth*, SALON.COM, May 27, 2000, *at* http://dir.salon.com/tech/view/2000/03/27/vranesevich/index.html.

104. Maggie Shiels, *Hackers Offered $1m To Reach Final Frontier*, HERALD (Glasgow), Apr. 18, 2001, at 21; Damien Pearse, *Hackers Compete in High-Tech Cyber Contest*, PRESS ASS'N, Apr. 22, 2001, LEXIS, Nexis Library, Wire Service Stories File; *Uncompromised $100,000 E-Security Challenge To Be Retired at DEFCON 2001*, BUS. WIRE, June 28, 2001, LEXIS, Nexis Library, Business Wire File.

105. *Uncompromised $100,000 E-Security Challenge To Be Retired at DEFCON 2001*, *supra* note 104.

106. *See, e.g.*, George V. Hulme, *Hacking Contest Reveals Solaris Vulnerability*, TECHWEB, Apr. 26, 2001, *at* http://www.techweb.com/wire/story/TWB20010425S0009; Matt Loney, *$100K Hacking Contest Ends in Free-for-All*, ZDNET NEWS, June 3, 2002, *at* http://zdnet.com.com/2100-1105-930689.html; Stuart McClure & Joel Scambray, *Hacking Contest Spotlights Many Ways To Attack Web Sites*, CNN.COM, Nov. 3, 1999, *at* http://www.cnn.com/TECH/computing/9911/03/hack.contest.idg/.

are annual affairs.[107] Companies continue to put contests to new uses. Early last year, the search engine Google announced a programming contest to develop software,[108] and Microsoft challenged hackers in order to test its software's security.[109]

Hacker contests deserve greater attention than they have garnered in the literature on computer crime. The market has turned hackers' competitive motivations to productive use, both as an advertising strategy and as a means of developing new products. The question arises whether the contests could be harnessed in a more formal, institutionalized fashion. Private industry stands to learn some lessons from the software market if it hopes to deter computer crime. The following Section of this Note outlines a proposed system of institutionalized contests or "hack-in days" sponsored by private companies to channel hacker activity. Through a regular series of contests, the Note argues, society can harness hacker motivations to deter computer crime while gaining a number of social benefits.

The security challenges are not structured to serve this function. First, although there are many contests, they remain infrequent. In order to emphasize the difference between illegal hacking and hacking within a contest's "safe harbor," a regular system of contests is necessary. Second, the security contests' infrequency and lack of systemization fail to discourage hitting other targets. With long lags between one contest and the next, these competitions fail to engage hackers consistently and may result in new "noise." By providing incentives to, and spawning interest in, hacking without creating a consistent legal outlet for those activities, these contests may increase overall hacking levels and may even attract new people to hacking.[110] In the absence of an approved contest space that is consistently available, these new hackers may engage in random hacking, benign or otherwise, raising targets' security and monitoring costs. A

107. Linda Wertheimer & Jason Beaubien, *Open Hack Competition Which Offers $50,000 to Anyone Who Can Hack into a Fake E-Commerce Web Site Set Up for the Contest*, Jan. 17, 2001, LEXIS, Nexis Library, NPR File. DataFort recently sponsored its second annual contest. DataFort, *at* http://hack.datafort.net (last visited Feb. 15, 2003).

108. John Borland, *Googly One: Search Site Offers Cash for Coding*, CANBERRA TIMES, Feb. 11, 2002, at A15.

109. Matthew W. Beale, *Microsoft Issues Open Challenge to Hackers*, E-COM. TIMES, Aug. 6, 1999, *at* http://www.ecommercetimes.com/perl/story/937.html.

110. Evidence indicates that instances of random hacking, as opposed to hacking within specified boundaries, lead to more hack attacks. Suddenly aware of Internet vulnerabilities, hacking victims themselves often begin to hack out of curiosity or out of a new awareness that hacking is easy. For example, after one such victim had his home computer hacked, he began to hack other computers, going so far as to contact his hacker for advice. *See* Peter Lewis, *High-Speed Internet Technologies Have Enabled an Increase of Electronic Security Risks for the Public*, SEATTLE TIMES, Dec. 12, 1999, at E1. If infrequent contests raise the incidence of overall random hacking activity by failing to provide a consistent outlet, one can imagine that this behavior might cascade as more targets are hacked and subsequently take up hacking.

system of frequent and well-publicized contests could absorb much of this random hacking.

Third, the security contests are completely anonymous. The company has a strong endorsement if it can claim that the most notorious hackers failed to breach its security. While these conditions provide fodder for advertisements, allowing companies to claim that their products withstood a rigorous public test, they fail to differentiate between acceptable and unacceptable hacking. The security contests implicitly sanction illegal hacking. Without such hacking, security companies would have no market. They stand to benefit from a hacking "arms race" and continued illegal hacking.

Finally, a number of sites will not buy security products, and the security contests may indirectly divert hackers toward those most vulnerable sites. More than anything, the security-sponsored challenges may be a warning to commercial site operators to buy protective software.

These complaints are easily summarized: The security contests make no expressive statement about the difference between legal and illegal hacking. By conflating the two, these contests do little to deter hacking. Contests can be designed, however, to produce a new hacker ethic that will deter computer crime.

B. *A Proposed Framework for Hacking Contests*

A contest designed to shape preferences and deter computer crime must confront several essential issues. First, it must clearly demarcate socially acceptable hacking from illegal hacking. If rewards and sanctions are to be effective, they must mutually reinforce each other as part of an interconnected whole. Second, for the reward to be an adequate incentive, it has to be publicized and alluring enough to induce hackers to participate.[111] Attracting all types of hackers will be a great challenge, and a balance must be struck in this regard—contests must be structured to be in the best interests of hackers, companies, and deterrence. Government may have a role to play to create these conditions. Finally, measures must be taken to authenticate participants' identities without dissuading them from competing. This Section seeks to develop a framework for thinking about the issues and to suggest some directions the contests could take.

111. *See* BENTHAM, *supra* note 67, at 224-25 (discussing motives as necessary to the force of law).

1. *The Model*

To help deter criminal hacking, firms could create a series of "hack-in" days, allowing hackers to hack their sites to expose vulnerabilities. The contest could be designed as a game or as a more serious security exercise. While the game model might not appeal to older hackers and would not reinforce the old hacker principle of improving code, it may be an appropriate educational tool for young hackers. Alternatively, the sponsoring firm could stage a dummy site—on which sensitive information would have been secured or removed—and invite hackers to break the code. Design choices should take into consideration the targeted audience and the intended goal.

A requirement of contest entry would be that the winners refrain from publicly revealing how they cracked the site.[112] Another possibility would be to require winners to repair the security holes they uncovered. (Arguably, hackers would have an incentive to do a good job, since their reputation would be on the line in the next competition involving that site.) Despite evidence indicating that some hackers are interested in actually creating secure networks as much as in deconstructing vulnerabilities,[113] this approach may not win hacker support. Alternatively, the contest could be monitored as a "honeypot"[114] so that winning methods could be recorded and technological vulnerabilities repaired.[115] Sites should remove all

112. Firms could thus avoid the problem that arose when Princeton professor Edward W. Felten won a contest by cracking digital music copy-protection schemes. Instead of claiming the prize, Felten published a paper explaining how he broke the code. *A "Speed Bump" vs. Music Copying: Master Cryptographer—and Code Cracker—Edward Felten Says Technology Isn't the Answer to Digital Copyright Violations*, BUS. WK. ONLINE, Jan. 9, 2002, *at* http://www.businessweek.com/bwdaily/dnflash/jan2002/nf2002019_7170.htm.

113. *See, e.g.*, Gottlieb, *supra* note 88, at 35-36 (reporting a hacker's dismay at the suggestion that he should actually "design a more secure version" rather than simply uncover and report existing security flaws); Messmer, *supra* note 88 (describing a company run by hackers that tests corporate networks for vulnerabilities and advises firms how to secure them).

114. Andrew Brandt, *Decoy PCs Give Hackers a Security Lesson*, CNN.COM, July 17, 2001, *at* http://www.cnn.com/2001/TECH/Internet/07/17/honeynet.project.idg/index.html (describing the benefits accruing to security experts from monitoring hackers' attempts to crack security through a network of PCs dubbed "honeypots"—networked PCs in various states of security that have been installed such that researchers can monitor attacks without being noticed by hackers); Mathew Schwartz, *Networks Use "Honeypots" To Catch an Online Thief*, CNN.COM, Apr. 4, 2001, *at* http://www.cnn.com/2001/TECH/internet/04/04/trap.a.thief.idg/index.html.

115. One of these or some analogous method will be essential to ensure that the contests actually result in increasingly secure websites. Hackers are better placed than law enforcement, or even Internet security professionals, to know how to make computer crime more difficult. Targets must tap into hackers' knowledge to help design better computer systems and prevent crimes. As Katyal explains:

> Because cybercrime is so easy to commit, and much of the knowledge needed to make it more difficult resides in private hands, government must devise methods to extract such information from criminals . . . . The use of informants to help design better computer systems and prevent crimes from occurring . . . portends a proactive, not a reactive, model of law enforcement.

Katyal, *supra* note 8, at 1034.

proprietary and private information from the "open zone" so as not to compromise themselves or their clients. Participating hackers might also be required to sign a hacker code of ethics resembling the older codes.[116] The code should focus on values like learning, understanding code, helping to create a secure technological infrastructure, and forswearing destruction.

An effective contest system must have regular and frequent competitions. Firms should organize and cooperate, creating a calendar by which different firms would take on the target role for different contests. As noted below, all participating firms need not sponsor their sites for contests. They may play other roles. Potential hacking victims already have incentives to organize and develop strategies to deter computer crime, given technical difficulties and the fact that law enforcement has proved unreliable.[117] Firms are likely to gain from the cooperative exchange of information and by mutually supporting efforts to deter computer crime, since each instance of crime has system-wide effects.[118] Participating firms could contribute to a pool used to pay for the contests, including the rewards offered, although monetary prizes may prove less necessary than reputational and legitimation incentives to encourage hacker participation. To reduce the cost to firms, government may play a role either by giving tax benefits to participants or by lowering e-commerce insurance rates for participating firms.[119]

While society would incur some deadweight loss from running the competitions, the contests should generate benefits that justify the expenditures. Computer crime cost about $250 million in 1998[120] and jumped to more than $375 million in 2001.[121] During this period, law

116. *See, e.g.*, LEVY, *supra* note 84, at 27-36.

117. Michael E. O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 281 (2000) ("Even otherwise natural competitors have an interest in maintaining secure transactions because each player is potentially vulnerable to a cyber-attack."); Ellen Messmer, *Web Sites Unite To Fight Denial-of-Service War*, NETWORK WORLD, Sept. 25, 2000, *available at* http://www.nwfusion.com/news/2000/0925userdefense.html.

118. O'Neill, *supra* note 117, at 281; Katie Hafner & John Biggs, *In Net Attacks, Defining the Right To Know*, N.Y. TIMES, Jan. 30, 2003, at G1.

119. The contests will be in the interest of past and potential targets of computer crime. In addition to a smaller incidence of computer crime, government may provide some incentives to participate. Participating firms may be rewarded by (1) receiving special tax breaks, and (2) benefiting from stricter than average penalties for computer crimes committed against them, resulting in greater deterrence. *See* Subsection III.B.2. As a negative sanction giving firms an incentive to participate, government could further require nonparticipating firms to pay higher Internet insurance premiums.

120. Crista Souza, *High-Tech Crime down 75% Since 1996*, ELECTRONIC BUYERS' NEWS, Mar. 18, 1999, *at* http://ebnews.com/showArticle.jhtml?articleID=2902875.

121. Thurston Hatcher, *Survey: Costs of Computer Security Breaches Soar*, CNN.COM, Mar. 12, 2001, *at* http://www.cnn.com/2001/TECH/Internet/03/12/csi.fbi.hacking.report/index.html (reporting that both the frequency and cost of computer security breaches had increased dramatically between 1998 and 2001).

enforcement expenditures increased[122] at the same time that the Internet security industry experienced a boom.[123] In 2000, private companies spent an estimated $300 billion in private enforcement efforts against hackers and viruses.[124] The combined cost of computer crime and governmental and private defense measures is exorbitant when measured against results. To the extent that competitions channel hacking away from criminal conduct and decrease cybercrime's cost to firms, contests should help pay for themselves. Individual target firms would not absorb all of the costs of developing a competition infrastructure. Just as a market has developed for security software, a market would likely develop for designing and promoting "hack-in" contests, creating competition and economies of scale.

2. *The Role for Government*

The argument thus far has focused on private, noncriminal measures to deter computer crime. While private ordering can provide essential supplements to deterrence via the criminal law, it may not generate these measures on its own. Government must play a role in reducing the cost of organizing contests. Four issues justify a limited role for government to induce contest participation.

First, existing market incentives encourage firms to buy security software and employ private investigators to attract customers and keep electronic vulnerabilities out of the public eye. Firms already engaged in these efforts may be reticent to support hacking tournaments. This is a collective action problem since, if the contests are to be effective, a number of participants are necessary. By subsidizing and helping to design the first contests, or even providing tax breaks or insurance subsidies to firms that participate,[125] government can overcome the collective action problem and make participation cheaper for firms.

Second, the failure of law enforcement to deter computer crime has led to the privatization of enforcement.[126] Security firms that track hackers without publicizing either the pursuit or identification of the culprit are an attractive alternative to police intervention, both because they are effective

122. Scott Harris, *Ashcroft Sets Sights on Cybercrime*, CNN.COM, July 24, 2001, *at* http://www.cnn.com/2001/TECH/internet/07/24/cyber.sheriff.idg/index.html.

123. Geoffrey Nairn, *Secrets of Security Success*, FIN. TIMES, Sept. 5, 2001, Special Section, at 2 ("In an IT industry laid low by profit warnings and lay-offs, internet security is seen as one of the few bright spots due to the supposedly recession-proof qualities of the sector.").

124. Anthony Shadid, *Fight Against Cybercrime Stalls as Focus Stays on "Putting Out Fires,"* BOSTON GLOBE, Mar. 21, 2001, at D1.

125. *See supra* note 119 and accompanying text.

126. Rustad, *supra* note 5, at 100-02 (arguing that law enforcement has failed to keep pace with cybercrime and that private enforcement is rapidly growing to fill this gap).

and because they do not expose firms to market punishment.[127] While these private mechanisms help individual firms, they do not provide general social deterrence. Government may play a role in encouraging mechanisms of deterrence with more generalized social value, like competitions.

Third, the details of the competitions are important. Government might implement baseline regulations so that contest designs do not produce crime instead of deterrence. For example, the space opened to hack-in contests must be strictly controlled so that proprietary information is not endangered. To prevent this and other potential harms from arising from the contest, government can set standards, perhaps in the form of guidelines issued by the Attorney General, with which all federally recognized contests must comply.

Finally, government must play a role because the tournaments' success depends on private and public coordination. Criminal penalties and penalty enhancements must reinforce the contest structure. Three policies would contribute to this mutual reinforcement. First, Congress should maintain strong criminal penalties outside of the contest context. Second, Congress should enact penalty enhancements for those who participate in a contest and are later convicted of computer crime. Finally, Congress should also enact penalty enhancements for illegal hacking on sites that are contest participants. This last policy would provide a further incentive for firms to participate.

Two approaches to penalizing attacks on contest participants are possible. First, contest participants could choose whether or not to post warnings that penalty enhancements apply to hacking on their sites. (The enhancements would not apply to hacking on nonparticipating sites, which should be distinguished from both contest sponsors and participants that play supporting roles.) Keeping some precautions unobservable—allowing the enhancement to apply even where the participant did not post a warning—would produce social benefits. If hackers were aware that enhanced penalties applied to hacking on some sites but could not determine which sites carried the greater risk, hackers could not be selective when choosing targets and would likely be more generally deterred than if they could clearly identify the riskiest sites.[128] While this "invisibility" approach would provide general deterrence, it could result in severe penalties for the unwary.

127. Friedman & Bissinger, *supra* note 5, at 2 (noting that notifying the authorities advertises the company's vulnerability to hackers); Rustad, *supra* note 5, at 100 ("Private enforcement in the form of 'E-cops' is already becoming well established on the Internet, as many American Internet companies are skeptical about the role of government in detecting and punishing hackers.").

128. For more discussion on invisible precautions and generalized deterrence, see *infra* notes 141-143 and accompanying text.

A second approach avoids overpenalizing the unsophisticated by placing warnings on all participating websites. Nonparticipating sites would not be prohibited from posting warnings, however, and may even be encouraged to do so. As a matter of self-interest, nonparticipating sites should have an adequate incentive to post a warning. Widespread use of such warnings should both produce general deterrence and increase the quantum of site-specific deterrence for each individual site that posts a warning, whether or not it has participated in the contests. Government should encourage participating and nonparticipating sites alike to post warnings by making these incentives known, communicating them to website managers and firms. Sites could then choose to participate in the contests as sponsors or supporting partners, to post a warning, or to do nothing at all. What is important is that they make an informed choice.

In order to be effective, the warnings must have essentially similar language. Firms that have participated in the contests would likely prefer to have specific warnings stating that enhancements apply to hacking on their sites. If nonparticipating sites could only post warnings in more general language, hackers could distinguish participating from nonparticipating sites and general deterrence would be lost. Thus, government should encourage all firms to use severe warning language and could even draft boilerplate warnings that all sites could use.[129]

Government could more actively encourage sites to post warnings, considering the general social value that would result from widespread posting. Since sites would already have an adequate incentive to post warnings that require negligible costs, however, government need not provide further incentives. Simply communicating the incentives to sites should be sufficient. This approach may, however, have some undesirable consequences. The strongest argument in favor of instituting a posting requirement is that, if posting is not uniform, hackers may substitute toward sites that do not have warnings. These sites are likely to be predominantly small, unsophisticated, and perhaps unaware that they may be targeted by

129. That government would encourage sites to post misleading warnings—warnings that mislead hackers to believe that penalty enhancements will apply to hacking on a particular site—would not create a problem of false advertising or false statement. Rules on false advertising are designed to regulate statements about commodities and employment in order to protect consumers and employees. *See, e.g.*, 15 U.S.C. § 1125(a) (1998) (prohibiting false statements in connection with commercial transactions that are likely to mislead consumers). The paradigmatic dangers underlying false advertisement—taking advantage of the unwary, the innocent, and the misled—are not implicated by the false warnings at issue here. The warnings would not encourage anyone to buy a product that has been misrepresented. Rather, they would seek to deter criminal behavior. Far from undermining the policy that animates regulation of false advertising, government encouragement of these warnings would reinforce it, protecting consumers from being harmed by illegal hacking. Moreover, rather than penalizing hackers unfairly, the warnings would provide heightened notice of the penal consequences that could result from hacking activities.

hackers.[130] To avoid this risk, government could institute a posting requirement, requiring all sites to use the same general warning language.

Three categories of actors would thus post warnings: (1) contest sponsors, (2) "hidden" supporting partners who have not actually sponsored a contest, and (3) sites that have not participated in the contests in any way. The enhancement would only apply to hacking on those sites that have a visible warning and are actual participants—categories (1) and (2). Under this "facade visibility" approach, government could both give unwary hackers fair warning about penalty enhancements and provide general deterrence by failing to clearly distinguish protected from unprotected sites. While the burden to add postings would fall on individual sites in the absence of a posting requirement, these sites would have an adequate incentive to do so or to advertise themselves to hackers as preferable targets.

The CFAA should be amended to encompass these enhancements for crimes committed by or against contest participants. A number of activities are already criminal under 18 U.S.C. § 1030(a), including knowingly accessing a computer and obtaining information that has been determined by the government to require protection for reasons of national defense or foreign relations, intentionally accessing a computer and obtaining restricted information, illegally accessing government computers, accessing a protected computer with intent to defraud, damaging computer networks, trafficking in passwords, and threatening to cause damage to a protected computer. In addition to those activities already criminal under the Act, subsection (a) should be amended to include the following language so that illegal hacking in relation to contests is explicitly punishable:

> (a) Whoever—
>
> (8)(A) having participated in a registered online hacking contest commits any of the violations listed under subsection (a); or
>
> (B) whether or not they have participated in a registered online hacking contest, commits any of the violations listed under subsection (a) against an individual or entity that has participated as a sponsor or a supporting partner in any such contest and posted a clearly visible statement to that effect on its website;
>
> shall be punished as provided in subsection (c) of this section.

130. To the extent that hackers are motivated by challenge or reputation, however, such sites may not be attractive targets. *Cf.* Louise Kehoe, *Hackers Hit AOL Cybervirgins*, FIN. TIMES, June 30, 1997, at 3 (noting that AOL users had been targeted in a string of hacking attacks "because the easy-to-use online service appeals to new and relatively unsophisticated internet users").

These new provisions would both protect contest sponsors and deter contest participants from engaging in random hacking by specifically criminalizing hacking with a contest nexus. Penalty enhancements should attach to such hacking to emphasize the "safe harbor" nature of the contests. Subsection (c) of 18 U.S.C. § 1030 currently provides for a fine, imprisonment, or both for violations of the Act. These penalties are of varying severity depending on the provision violated. Subsection (c) could be amended to include the following language targeting hacking with a contest nexus:

> (c) The punishment for an offense under subsection (a) or (b) of this section is—
>
> (5) a penalty enhancement, not more than doubling the statutory penalty, in the form of an increased fine, increased imprisonment, or both, in the case of an offense under subsection (a)(8)(A) or (a)(8)(B) of this title.

Finally, to ensure that the contest designs are adequately tailored to produce deterrence, the government should create standards with which the contests must comply. Current subsection (e) of § 1030, which defines the terms used in the statute, would become subsection (f), and new subsection (e) would read:

> (e) In order for the provisions of this section to apply, online hacking contests shall be registered in accordance with guidelines issued by the Attorney General.

Government cooperation is necessary to create the conditions under which contests can successfully enhance the criminal law, and these amendments to current law should ensure that the contests effectively deter crime.

As argued above, on its own, government action has produced little deterrence in the context of computer crime. Government can enhance the contests' deterrent effect, however, by reducing the cost of organizing contests, regulating contest design, and creating linkages between contests and the criminal law. Put more simply, government can play a supporting role, acting as a catalyst to help private actors deter computer crime.[131]

131. William A. Reinsch, Under Secretary of Commerce, stated:
> With respect to prevention and the development of more comprehensive security measures, the government can best play a supporting role. The infrastructure at risk is owned and operated by the private sector. Inevitably, it will be they who must work together to take the steps necessary to protect themselves.

While private parties must take steps to deter hacking, government has a role to play to ensure that private ordering is effective.

3. *Rewards and Penalties*

Much of the economic literature on crime focuses on the probability of punishment.[132] One might argue that the reward model, offering status incentives and monetary prizes to contest winners, is flawed because the number of winners could never match the number of hackers who are caught. From this perspective, the relatively low probability of reward would not have much deterrent effect. The argument ignores those hackers who would be content with a legitimate venue for hacking and for whom the contests would provide a satisfying alternative to illegal hacking. As for hackers concerned with peer recognition, the argument is vulnerable on two counts. First, the probability of capture for a computer crime is already quite low, minimizing the deterrent power of criminal sanction. Thus, even a small probability of reward may be as much a deterrent as the probability of being punished.[133] Moreover, empirical studies indicate that low probabilities are often conceptually inflated, explaining why people are willing repeatedly to play the lottery.[134]

Second, one can design a model where the probability of winning is not low. Each contest could be split into a number of parts with a winner designated for each component. Alternatively, the contest could be timed, with the top ten finishers declared winners. In either case, a cumulative ranking system of the top 100 or 200 hackers could be posted on a centralized site to give hackers a psychic incentive to compete even if they cannot be *the* winner. With either system, winners' names must be published promptly. While winners will also receive monetary rewards, or perhaps even jobs,[135] emphasis should be placed on an effective campaign

> The government can help. We can identify problems and publicize them. We can encourage planning, promote research and development, convene meetings. In short, we can act as a catalyst.

See Cybercrime Hearing, *supra* note 27, at 38.

132. *See, e.g.*, Becker, *supra* note 10.

133. *See* Tittle, *supra* note 80, at 405 (arguing that behavior can be influenced "by fear of punishment or anticipation of reward produced by observing others being punished or rewarded").

134. Daniel Kahneman & Amos Tversky, *The Psychology of Preferences*, SCI. AM., Jan. 1982, at 160, 164.

135. The security-contest sponsors learned quickly the importance of tailoring the prize to the audience. *See supra* notes 104-107 and accompanying text. While rewards should focus on bragging rights, other incentives could also be employed. In addition to monetary rewards, contests could be structured as a hiring mechanism. *See* Daffyd Roderick Manila, *Hacker's Paradise*, TIME ASIA, Apr. 16, 2002, *at* http://www.time.com/time/asia/digital/magazine/0,9754,105665,00.html (describing how Filipinos with technical expertise resort to computer crime because they cannot find technology jobs); Thurman, *supra* note 101 (noting the willingness of one security manager to hire hacker talent). The socially legitimating function of

to publicize their names or pseudonyms. (As argued below, although it is essential to verify identity for administrative purposes, hackers could create their own contest identities.) An advertising strategy that persuasively characterizes these rankings not only as an accurate but as the definitive reflection of hacker skill would strengthen the contest's force.

It is important to emphasize that the contests should not replace criminal sanctions. Punishment must be integrated with positive incentives, and the interaction between the two will deter computer crime. Punishments are necessary to ensure that reputational gains derived from the contest are only available to participants. It is essential that the contests become the sole, or at least the primary, source of hacking reputation and bragging rights. Defectors who seek bragging rights outside of the contests must be given a negative incentive.[136] The criminal law should not only penalize crimes connected to contests, however. It should also create shaming techniques designed to delegitimize hackers who brag about their illegal exploits.[137] While these proposals will not enhance enforcement, the law's expressive function is most important in this context. The goal is that criminal hacking should no longer be associated with reputation as a skillful hacker. As long as the criminal law reduces the psychic benefits derived from illegal hacking, creating a stigmatizing effect, high enforcement levels are not necessary. Publicity campaigns encouraging hackers who seek prestige to participate in contests may compensate for suboptimal enforcement. In this manner, reward and punishment would work together to deter computer crime.

Penalty enhancements are a key element of the proposal. Social scientists have advocated keying the severity of punishment to the level of victim precautions,[138] and legal scholars have developed a theory of when sentencing enhancements should apply.[139] Katyal argues that enhancements are justified when targeted at harmful applications of conduct or technologies that have "dual uses."[140] Contests create a dual use situation—hacking is viewed as socially beneficial within a demarcated space and

hacking in specially demarcated spaces should be an incentive for hackers who see themselves as providing a public good.

136. For discussion of penalties for hacking outside of the contest framework, see *supra* Subsection III.B.2.

137. In addition to being fined or imprisoned, those convicted of computer crime in connection with a contest could be shamed. The Justice Department could maintain a website (linked to popular hacking websites) posting hackers who have been caught and prosecuted to show that the contests are a better source of prestige than illegal hacking. *See infra* text accompanying notes 198-199 (describing how bragging about extra-contest hacking often leads to identification and prosecution).

138. *See* Omri Ben-Shahar & Alon Harel, *Blaming the Victim: Optimal Incentives for Private Precautions Against Crime*, 11 J.L. ECON. & ORG. 434, 444 (1995) (arguing that where victims have not taken adequate precautions, criminal punishment should be lighter).

139. *See* Katyal, *supra* note 8, at 1061-63.

140. *See id*.

criminal outside that space. When hackers attack participating sites or participate in contests themselves before committing unauthorized intrusions, they abuse the trust that is established by the contest and desanctify a space created to cultivate social norms. The penalty enhancement is one means of ostracizing those who interrupt the process of norm reconstruction.

Applying differential penalties depending on the victim's behavior—whether or not they have sponsored a contest—raises the visibility/invisibility question.[141] If only firms that actually sponsor contests benefit from the enhanced penalties, the rule may cause substitution effects—hackers may simply choose other targets.[142] Allowing some firms to be *invisible* partners may have more general deterrent effects. If a hacker cannot be sure whether hacking into a particular firm would carry a greater penalty, he may be deterred more than by clearly labeled risky targets.[143] As noted above, however, such a rule may result in overpenalizing unsophisticated hackers.[144] Contests can fairly accommodate this invisibility interest through the "facade visibility" approach that encourages all sites, whether participants or not, to post a warning that a severe penalty enhancement may apply for attacks on that site.[145] Under this approach, the consortium of participating firms could play a number of roles. Not all firms need to sponsor their site as the locus of the contest—they could provide funding, technological expertise, and the like as silent partners. Hacking into any of these firms' sites would trigger the penalty enhancement as long as they had posted warnings. For these specially tailored legal sanctions to work properly, however, the enhancements, as well as the fact that "hidden partners" and dummy warnings exist, must be clearly publicized.

Facade visibility achieves the same policy goal as invisibility by shifting the baseline. Rather than beginning with uniform lack of warning and relying on unobservable precautions to provide general deterrence, with facade visibility most actors would have visible warnings while only some actually would have taken precautions. In both cases, hackers would face

141. *See* Ben-Shahar & Harel, *supra* note 138, at 452 (noting that where victim precautions are unobservable, criminals cannot be as selective and run the risk of targeting a protected victim, which results in greater deterrence).

142. *See* Katyal, *supra* note 75, at 2387.

143. Applying penalty enhancements for those who hack into invisible contest partner sites would not present a Fifth Amendment due process problem. Hackers would already be aware that hacking into the site is a criminal act. Thus, there is no notice issue as to the substantive crime itself, only the magnitude of the penalty, which does not rise to the level of a due process concern. *Compare* Muscarello v. United States, 524 U.S. 125, 126, 138-39 (1998) (declining to apply the rule of lenity and to construe a penalty-enhancement provision in favor of the defendant), *with* McNally v. United States, 483 U.S. 350, 359-60 (1987) (construing an ambiguous substantive criminal statute narrowly and in favor of the defendant).

144. *See supra* Subsection III.B.2.

145. *See supra* Subsection III.B.2.

uncertainty, could not be selective in choosing targets, and would run the risk of targeting a protected victim. Such uncertainty should produce significant general deterrence.

Invisibility and facade visibility create their own difficulties. One side effect might be to cause crime of a different sort. For example, if hidden technology such as LoJack reduces the incidence of car theft, Seven-Eleven robberies may increase.[146] While invisible risk may encourage hackers motivated by profit to engage in other crimes where the level of risk is more apparent, the contest model accounts for the substitution possibility with respect to unauthorized access by providing its own legal substitution. If the contest is properly designed, the utility a hacker derives from participating in it should be at least equal to that derived from unregulated hacking. At the same time that it creates a legal channel for the prohibited behavior, the contest attempts to create preferences for that legal conduct over illegal computer crimes. Thus, a contest that allows a number of potential victims to keep their precautions unobservable will likely produce deterrence that is socially beneficial without causing target diversion or substitution of more serious crimes.

As noted above, penalty enhancements should be well publicized. Strengthened penalties are meant to enfeeble the "black market" where participants might develop hacking expertise or put their skills to illicit uses. These measures could be strengthened by a "three strikes" rule. Hackers implicated in a specified number of offenses would not be able to compete. To prevent some hackers from being locked out entirely, a date could be set so that everyone would begin with a blank slate. Alternatively, hackers could take away a strike for each public interest job they do (as long as they do not add any new strikes), such as beefing up a site's security or turning state's evidence to prosecute other crimes.

4. *Who Will Participate?*

One of the toughest questions contest developers must confront is the question of who will participate. Hack-in contests should offer hackers a legal outlet that responds to a number of the factors that motivate them. A comprehensive study by the Boston Consulting Group recently surveyed hackers to determine the most common motivations.[147] Hackers identified intellectual stimulation and improving computer skills as the top two

146. *See* Ian Ayres & Steven D. Levitt, *Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of LoJack*, 113 Q.J. ECON. 43 (1998). Ayres and Levitt's work measures whether the LoJack auto-theft device increases the commission of other crimes, such as robbery.

147. Karim R. Lakhani et al., The Boston Consulting Group Hacker Survey 12 (July 24, 2002), *at* http://www.osdn.com/bcg/BCGHACKERSURVEY-0.73.pdf.

motivating factors.[148] Anecdotal evidence indicates that hackers are also motivated by a competitive urge to earn peer recognition and bragging rights.[149] Hack-in contests should create a legally structured space that accounts for each of these motivations. In the contests, hackers could pursue their curiosity and build skills. As noted above, the contests could also be structured to provide a source of reputation and bragging rights. Hackers might have a more positive attitude toward these contests than toward sanctions, which they may take pleasure in flaunting.[150] Whatever the motivation, targeting young hackers at developmental stages is wise.[151] The contests should target seasoned hackers as well. Appealing to reputation has the potential to rehabilitate experienced hackers. Those who hack out of either curiosity or to build computer skills could also find satisfaction in the contests without resorting to criminal activities. Contests would not provide a viable substitute for all hacking, however. Politically or profit-motivated hacks would not be deterred. As noted in the Introduction, the contest is tailored to directly deter simple unauthorized access, not these other forms of computer crime.

Security contest sponsors have faced two serious issues in motivating hackers to participate, though neither concern implicates hackers seeking a legitimate venue for hacking. First, criminal-minded hackers might not want to help the security industry by participating in such a contest.[152]

148. *Id*.

149. *See* TAYLOR, *supra* note 9, at 59 (finding that hackers seek peer recognition and respect). Hackers are renowned braggers. A number of newsgroups, particularly alt.2600.hackers, are frequented by hackers bragging about their accomplishments. *See, e.g.*, ERIC S. RAYMOND, *Homesteading the Noosphere*, *in* THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY 65, 89 (2001) ("Having established that prestige is central to the hacker culture's reward mechanisms . . . [t]he best brag is code that 'just works', and that any competent programmer can see is good stuff."), *available at* http://www.firstmonday.dk/issues/issue3_10/raymond/; Bruce Sterling, *Good Cop, Bad Hacker*, WIRED-MAG., May 1995, at 122, 124 ("Hackers will also talk to journalists. Hackers brag all the time."). Law enforcement often captures culprits because they have bragged. Ariana Eunjung Cha & John Schwartz, *More Big Web Sites Hit by Hackers*, WASH. POST, Feb. 9, 2000, at E1 (quoting a security industry employee who stated that most criminal hackers are caught because they cannot resist bragging); Sascha Segan, *Tracking "Mafiaboy's" Steps*, ABCNEWS.COM, Apr. 20, 2000, *at* http://abcnews.go.com/sections/tech/DailyNews/webattacks000420.html (quoting Quebec Inspector Yves Roussell, who stated that hackers "like to brag about their capability, their exploit[s]; they like to tell the public what they did").

150. *See, e.g.*, Bendavid, *supra* note 19 (describing hackers' taunts as they evade law enforcement).

151. *See* John Van Beveren, *A Conceptual Model of Hacker Development and Motivations*, 1 J. E-BUS. 1 (Dec. 2001), *at* http://www.ecob.iup.edu/jeb/December2001-issue/Beveren%20article2.pdf (tracing the development of new hackers and charting their motivations from tool kit/newbies into either cyberpunks or old-guard type hackers and finding that, as young hackers develop skill and experience, unauthorized intrusion committed by tool kit/newbies appears to be a gateway activity that could lead to either malicious or nonmalicious hacking).

152. Wertheimer & Beaubien, *supra* note 107.

Second, hackers who want bragging rights may wait until a site is declared invincible before trying to crack it, hoping to earn greater notoriety.[153]

As for the first issue, unlike the security contests meant to help sell products, the proposal here need not be framed as a boon to any industry. The contests should be characterized as a tool to increase Internet security generally, a goal with which many hackers are sympathetic. Skillful advertising should also present the contest as the definitive measure of hacker skill, emphasizing the rankings. It should stress that the best hackers in the world compete, prompting those who resist to participate out of hubris. These techniques would hopefully attract even the cleverest hackers who might otherwise be reluctant to participate.[154] Tough penalties and penalty enhancements may deter much of the postcontest, extralegal hacking, decreasing the chance that some hackers will wait until the tournament concludes to hack into the site.

While some hackers may find the contests overly artificial, private hack-in contests have elicited massive participation rates. In contrast to the counterculture point that participating in a contest could be seen as "selling out," a private contest last year received 20,000 attempts.[155] These numbers suggest that, if the contest is adequately challenging and involves real software or real networks, many hackers will be interested.

Anecdotal evidence reinforces the numbers, indicating that these competitions may actually appeal to hackers. One commentator contends that, given a legitimate venue or permission to hack, many hackers would not engage in illegal hacking.[156] Indeed, one hacker argues that, if hackers are given legitimate access to systems in order to explore and learn, "it would curb the urge to break into other sites."[157] The fact that the contest creates a legitimate hacking venue is essential. For many hackers, this legitimized space may be enough to turn them from illegal and socially deleterious hacking to hacking that has social benefits.[158]

153. *Id*.

154. *See Hackers Invited To Crack Newest Security System*, CHI. TRIB., Jan. 16, 2001, § 1, at 8 (noting that dangerous hackers often opt not to enter the security contests and have little interest in sharing their ability to break into sites).

155. *Uncompromised $100,000 E-Security Challenge To Be Retired at DEFCON 2001*, *supra* note 104.

156. TAYLOR, *supra* note 9, at 53 (referencing an e-mail interview with Dr. Fred Cohen).

157. *Id*. at 55 (quoting an interview with Chris Goggans).

158. The hack-in contest proposal is analogous to the approach a number of cities have adopted to deal with gang-related graffiti—creating mural programs to channel youth artistic talent into a product with community benefits. The first mural program in the country, in Philadelphia, enlisted young graffiti artists to replace graffiti with murals on condition that they agreed no longer to deface property. Jennifer Brown, *Philadelphia Murals Are Biographies of Its Neighborhoods*, CHI. TRIB., Oct. 30, 2000, § 5, at 2; Sue Halpern, *The Art of Change*, MOTHER JONES, July-Aug. 2002, at 30, 32. By 1991, seven years after the program's birth, less than one percent of the Philadelphia murals had been vandalized. Michel Marriott, *Public Art Tackles Graffiti, and Wins*, N.Y. TIMES, Sept. 13, 1991, at A14. The program has been replicated in a number of other cities, including San Diego, *see* City of San Diego, *at*

Apart from the question of how to attract hackers, there remains the issue of who should be allowed to compete. Ex-felons, those under criminal suspicion, those under indictment, and convicted criminals serving jail time, one might argue, should not be allowed to participate.[159] If any participants would be prone to developing skills that will be put to impermissible uses, this class of hackers runs the greatest risk. Judgment on the issue turns on the assessment of tournaments themselves. If they perform their intended functions, they will both create preferences for socially approved hacking and deter criminal activity. While the strongest impression is likely to be made on young hackers in their formative years, competitions have rehabilitative potential as well.[160] If, on the other hand, one views competitions as the breeding ground for cybercrime networks, criminal elements might best be excluded from participation.[161]

Some security companies have made their contests anonymous. Last year, one company, in an effort to attract hackers, stated that the first hacker to succeed would simply find a bank account number waiting for him.[162] A company more interested in advertising than nurturing social norms can afford to do this. Anonymity would not be desirable in the contest model proposed here, though pseudonymity is essential.[163] Pseudonyms are already prevalent in hacker culture,[164] so adopting them in competitions should not prove difficult.

http://www.sannet.gov/graffiti/school.shtml (last visited Dec. 29, 2002), Santa Fe, *see* City of Santa Fe Arts Comm'n, *at* www.cominguptaller.org/profile-add/pr-add02.htm (last visited Dec. 29, 2002), and Jersey City, *see* Pro Arts, *at* http://www.nices.com/proarts/mural.html (last visited Dec. 29, 2002). The sheer number of cities that have initiated mural programs is indicative of the programs' success, not only at reducing graffiti, but also at providing other, intangible benefits to urban environments. These successes suggest that, arguments about counterculture aside, programs designed to channel creative talents into constructive activities can replace, to a large extent, the destructive uses to which those talents had previously been put. The experiences of these cities indicate that hack-in contests, if well designed, can harness hackers' talents and put them to good uses by both engaging hacker interest and providing them with reputational payoffs.

159. The argument is stated here in its simplest terms. A more nuanced statement would take into consideration the kind of felony committed and the potential danger that could arise from allowing a particular class of felons to engage in permitted hacking. Prohibiting ex-felons or criminal suspects from participating in the contests may also raise the ex post facto issue.

160. To the extent that hackers seek social legitimation, peer recognition, or both, the contests could persuade these hackers to forgo criminal hacking.

161. *See infra* Section IV.B. Those hackers involved with the criminal justice system would already have some incentive to avoid illegal hacking outside of the competitions. They are more likely to be closely monitored and penalties are likely to be more severe the second or third time around.

162. Shiels, *supra* note 104.

163. Obtaining information about the person responsible for harmful behavior is impossible in an anonymous framework. Moreover, anonymity presents a moral hazard. Because individuals do not bear the reputational costs of their behavior, the aggregate amount of harmful behavior may increase. David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 142.

164. Rogers, *supra* note 76 (noting that hackers often use nicknames from science fiction or fantasy, reflecting the use of the computer as a means of escapism).

Compared to anonymity, pseudonyms "permit[] the accumulation of reputational capital and 'goodwill' over time in the pseudonym itself."[165] Pseudonymity must be regulated in the competitions, however, because its benefits depend on the development of the name in an historical context.[166] A nongovernmental third party, bound by strict privacy rules, could screen participants to ensure consistent use of a single pseudonym. Participants would only be required to reveal their pseudonyms, not their real names. Pseudonyms could help constitute a positive online identity that provides context-specific reputational effects as well as carry-over benefits beyond the contest. In other words, pseudonyms can contribute to the creation of positive social norms within the hacking community. Accumulation of reputational capital through pseudonyms is essential for bragging rights and criticism to be effective. Contest participants will build a reputation for skill that adheres to their chosen contest identity or pseudonym. While social legitimation may be enough to induce those hackers who would prefer to hack in legal venues to participate, this aspect of reputational capital, along with cash prizes, constitutes one of the primary incentives for hackers to compete. The combination of incentives and penalties described above, along with the benefits of pseudonymity, should allow for an inclusive participant list.

Efforts could also be made to encourage team participation in contests. The goal would be to decrease the Internet's isolating effect on hackers and to help reestablish the communal networks of the early hacker organizations. To the extent that such organizations could be supported through contests, positive norms and ethics could once again be reinforced through integrated social processes.

5. *Authenticating Identity*

In order for the contests to employ reputational incentives properly, participating firms must authenticate competitors' identities. Competing hackers who are able to "steal identities" would undermine the contests' legitimacy. While emphasizing bragging rights will give many hackers an incentive to be forthcoming with their identities, a digital signature along the lines Lessig describes would be useful.[167] A nongovernmental third party could be entrusted with issuing digital identification cards. Even vigilante hackers could register, provided that government would not have access to their information. The third party would be responsible for determining the participants' eligibility, and only the pseudonym would be

165. Post, *supra* note 163, at 142.

166. *Id*. at 154. If hackers could adopt different contest pseudonyms at will, the reputational value of pseudonymity would be lost.

167. *See* LESSIG, *supra* note 8, at 39.

transferred to the contest sponsor. As a final disincentive to identity falsification, participants discovered to have used fake identification should be prosecuted.

C. *Summary*

The proliferation of hacker competitions, both in hacker culture and as a tool of the technology industry, suggests that such competitions may have broader uses. Competitions may be relevant as a deterrent strategy to complement the criminal law. If competitions are to deter crime effectively, however, they must be carefully designed. Government may have a role to play, among other things, in reinforcing the contests with strong protections of contest sponsors and strict penalties on participants who engage in random hacking. A carefully designed contest should produce deterrence consistent with preference-shaping theory while capturing the benefits of limited decriminalization.

IV. EVALUATING THE CONTEST PROPOSAL

A. *Comparing Contests with the "Duty To Report"*

The contest proposal can capture the benefits of decriminalization while leaving the criminal law intact. These benefits are abundant. First, as hackers hack into contest sites, they will identify latent security flaws. The contests should be structured so that hackers are challenged to find such flaws. Once weaknesses have been identified, participating firms will repair the sites, ratcheting up Internet security. One can imagine a virtuous circle as hackers identify ever-smaller flaws in increasingly secure sites. Participating firms may even gain the advantage of claiming to consumers that their sites, having been subjected to rigorous testing, are the most secure.

Second, as contests help to disaggregate the hacker community and to destigmatize those hackers who do not have malicious intent, it is likely that trust among hackers, law enforcement officials, and security personnel will grow.[168] While elements of this trust are already visible as companies hire hacker "tiger teams" to test their systems' security,[169] contests may

168. Taylor has argued that strong pressures to treat all hacking as criminal have resulted in legislation that hackers think fails to deal with Internet security weaknesses that remain latent and untested. TAYLOR, *supra* note 9, at 123.

169. *See Could You Pass the Tiger Test?*, GUARDIAN (London), Mar. 9, 2000, at 12, *at* http://www.guardian.co.uk/print/0,3858,3971784,00.html; *When Is It Ethical To Hack?*, BUS. LINE, Aug. 5, 2002, LEXIS, Nexis Library, Global News Wire File.

help develop more structured "trusted relationships" as contests evolve into a formal, legitimized space where hackers work.

Third, as much "look-and-see" hacking, and some of the more outrageous hacking motivated by bragging rights, is channeled into contests, law enforcement resources are likely to be conserved. To the extent that these resources can be concentrated on the most flagrant instances of computer crime in effective ways, companies may become more willing to press cybercrime cases,[170] in turn strengthening enforcement of computer crime laws through experience.

Fourth, the contests would provide a forum for hackers to pursue their curiosity, to think creatively, and to make technological discoveries. This development of human capital and technological knowledge will create social benefits to the extent that hackers are no longer marginalized. Their new skills may be put to good uses as they find jobs in the technology industry or as they contribute to "creative compilations"—technologies or software produced through online experimentation and rigorous testing.[171]

Finally, as suggested above, the contests would also create conditions conducive to a broad-based discussion about Internet architecture and how its construction should proceed. To the extent that hackers are stigmatized, their knowledge of, and opinions about, the Internet remain on the margins of public debate. Without access to their knowledge, the public may not have the resources to critique developments in Internet architecture.[172] The contests provide a forum in which hackers may receive a voice as technological experts with valuable insights about the Internet that are relevant to the broader public.

170. While companies are reluctant to pursue cases and advertise their security vulnerabilities, companies' reticence also reflects a lack of faith in law enforcement. Anthony Stavrinos, *Police Launch Intelligence Network To Tackle Cybercrime*, AAP NEWSFEED, July 18, 2001, LEXIS, Nexis Library, AAP Newsfeed File (noting the lack of confidence in law enforcement); *see also Cybercrime Hearing*, *supra* note 27, at 70 (statement of Mark Rasch, Vice President, Cyberlaw, Global Integrity Corp.) ("[O]ne of the problems we have is a fundamental distrust between the commercial sector and law enforcement."); Rosenblatt, *supra* note 25, at 37 (arguing that police departments are poorly equipped to handle computer crime cases and fail to inspire confidence).

171. Linux is a prominent example of the kinds of benefits that can result when decentralized technological expertise is harnessed to produce public goods. *See, e.g.*, Declan McCullagh & Robert Zarate, *Super-Secure Linux, Inch by Inch*, WIRED NEWS, June 11, 2002, *at* http://www.wired.com/news/linux/0,1411,53004,00.html (noting the success of Security-Enhanced Linux, an Open Source product designed in large part by volunteer programmers, at countering attacks); *see also* Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 374 (2002) (generalizing from "the phenomenon of free software to suggest characteristics that make large-scale collaborations in many information production fields sustainable" and describing the benefits of "peer production").

172. *See* TAYLOR, *supra* note 9, at 123 (arguing that, because hackers have been marginalized, the public is left with inadequately secure networks).

Contests differ from the reporting rule—which presumes any instance of reported unauthorized access to be nonmalicious[173]—in that they set up a distinct "safe harbor" where hacking is allowed. This enables the contest proposal to avoid many of the difficulties of broader decriminalization proposals. Because intrusions into private networks outside of this specially created space are prohibited, the contest is more likely than the reporting rule to attach social meaning to hacking conduct and to shape preferences. Whereas the reporting rule poses serious concerns along four key dimensions, the contest proposal, by maintaining a prohibition on unregulated hacking, avoids these difficulties.

First, the reporting rule essentially permits hacking by subjecting it to a liability rule. Hackers have the choice of *pricing* their activity by determining when it is worthwhile to report and when it is not. The contest model does not allow such individual pricing. In the contest, only a narrow category of hacking is permitted in a specially demarcated space. Unlike the reporting rule, the contest model does not give hackers carte blanche to hack as long as they come clean after the fact.

Second, as a liability rule, the reporting rule permits legal breaches of privacy. The contest does not allow hackers to invade private networks. Since each participating firm is able to prepare before the contest begins, it will be able to protect both its customers' and its own privacy.

Third, the fact that all targets are not alike has important policy implications. Some targets could not accept a reporting rule, and they would have to be declared off-limits. This fact complicates the reporting rule and could be accommodated only with great difficulty. With contests, targets are self-selecting. They can choose how and when to open themselves to attack.

Fourth, under a reporting rule, small targets may not be able to defend against hacking as well as large companies that can purchase the most current security devices. Moreover, the reporting rule implicitly encourages ad hoc bargaining between companies and hackers who have breached security, an arrangement that favors larger companies. With the contest model, bargaining is standardized and up-front, eliminating the possibility for "green mail." The contest can also be designed to include small firms.[174]

Measured against the reporting rule, the contest model avoids many of its pitfalls. The reporting rule takes decriminalization too far. It fails to send a clear signal that hacking is criminally prohibited, essentially allowing hackers to self-regulate. The challenge is to determine whether the reporting rule's benefits—the advantages deriving from

173. *See supra* Section I.B (describing the reporting rule and providing a general critique of it).

174. *See supra* Subsection III.B.1.

decriminalization—could be captured through a more narrowly circumscribed decriminalization project, the regulated hack-in contest. Consistent with the insights of preference-shaping theory, contests can capture these benefits while maintaining a clear prohibition on criminal hacking.

In the contest model elaborated above, preference shaping that is begun through criminalization is reaffirmed through positive reinforcement for socially permissible hacking. A corollary to the limited, "safe harbor" decriminalization of the contest is the creation of positive incentives to obey the law, participate in the contests, and forsake criminal hacking. The contest gives those who hack for intellectual motivation or to improve their skill an incentive to hack not only in ways that they believe are socially beneficial, but also in ways that are publicly recognized as legitimate.[175] Likewise, the contests provide peer recognition to those motivated by status and reputation.[176] By channeling hacking into legal outlets, these positive incentives to engage in legal behavior can deter much criminal hacking.

Maintaining clear prohibitions on hacking outside of the contests, this limited decriminalization is wholly consistent with preference-shaping theory, which recognizes the preference-shaping power of both rewards and the criminal law.[177] Through the positive incentives noted above, regulated contests would not only channel activities in law-abiding directions, but they would also shape preferences by encouraging the development of positive social meanings for law-abiding conduct.[178] Positive incentives are necessary because, given the consequences of deviance labeling and the antiauthoritarian aspects of hacker culture, criminal sanctions alone could not do this.[179] Criminal penalties cannot harness the positive aspects of the hacker ethic and may even undermine them. The contest proposal provides a preference-shaping alternative in which deterrence is achieved both by providing clear criminal prohibitions and by nurturing hacker ethics.

175. Many hackers view themselves as making the Internet safer. *See, e.g.*, Catherine Therese Clarke, *From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191, 207 (1996) (arguing that hackers seek to improve the Internet and noting that "traditional hackers are not considered to be law breakers; their mens rea is presumed innocent"); John Markoff, *The New Watchdogs of Digital Commerce*, N.Y. TIMES, Oct. 16, 1995, at D1 (finding that hackers want to explore the Internet fully and eliminate "the flaws to create a perfect system"). Providing a space constructed around an articulation of hacking's benefits can serve an important legitimating function and may even create positive community norms. *See* TAYLOR, *supra* note 9, at 43-44 (arguing that "articulations of what it is to hack and why people do it may have a disproportionate role to play in community formation within the computer underground and in influencing the perceptions of those external to the activity").

176. *See supra* note 149 and accompanying text.

177. Dau-Schmidt, *supra* note 21, at 18.

178. *Id*.

179. *See supra* Section II.B.

The claim is not that the contests will deter computer crime altogether. An effective punishment regime could not do that. Rather, this Note modestly suggests that the contests may help determine what the range of normal behavior is, deterring much aberrant conduct. Remembering that it is an *interaction* of costs and rewards that shapes human behavior, we should note that the contest model is a *supplement* to criminal penalties.[180] Contests would shape preferences through the confluence of positive incentives to good conduct and penalties for criminal hacking. Computer crime is particularly ripe for this method of preference shaping given that hacker culture is already endowed with positive ethics that law should seek to reinforce.

B. *Potential Objections to the Contest Model and Responses*

Several objections that the tournaments will actually increase computer crime deserve consideration. Many of these objections overlook the current context in which hacking occurs, characterizing the dangers of continuing to rely on technological security and private enforcement measures as risks specific to the contests. Others misunderstand the relationship between unauthorized access, other computer crimes, and the contest framework. While superficially attractive, none of these objections is strong enough to reject the competitions.

First, some may argue that competitions would allow hackers to meet each other and band together, turning their abilities to illicit uses. Upon closer analysis, however, it is evident that tournaments would not provide new opportunities for hackers to create criminal networks. A number of fora already exist where hackers associate. Many hackers go to Las Vegas each year for the DEFCON conference where they trade methods and hone techniques.[181] During the rest of the year, hackers exchange tips in chatrooms.[182] Given contest pseudonymity, participants would have no new means of communication. The competitions would do little to create new opportunities for conspiracy. Even if tournaments did create the conditions for criminal networks, the tournaments should also make law enforcement's job easier. By allowing for the monitoring of contests and the surveillance of various hacker styles, competitions should lead to more effective target-hardening measures and should also familiarize law enforcement with hacker methods.[183]

180. For discussion on the interaction of rewards and punishments, see *supra* Subsection III.B.3.

181. Thurman, *supra* note 101.

182. *See supra* note 91.

183. *See* Brandt, *supra* note 114 (describing the benefits accruing to law enforcement from monitoring hackers' attempts to crack security). Monitoring may discourage some hackers from

Second, the tournaments may provide a venue where hackers can hone skills that will eventually be used to engage in criminal hacking. This concern—that hacking contests are like a "sandbox"—also proves illusory upon further analysis. First, rather than encouraging computer skills, competitions simply try to harness them. As noted above, numerous and easily accessible websites teach hacking skills.[184] It is not clear that tournaments would create new interest in hacking or develop new skills rather than channel potentially deviant behavior into positive outlets. Contests may, however, give hackers confidence in their abilities. This may not be a wholly negative development from a law enforcement perspective. As noted below, to the extent that such confidence leads to the boasting that often accompanies illegal hacking, law enforcement will be more effective. Second, it is worth repeating that the contests do not target profit or vandalism-motivated hacking.[185] Rather, they aim to provide a substitute for unauthorized access and to shape preferences among hackers engaged in these kinds of activities. If the contests are successful at creating preferences for such hacking among the targeted group, many participants will choose not to engage in criminal activities. Third, if the developmental theory of hacking is accurate,[186] the maturation from tool kit/newbie into cyberpunks or old-guard hackers depends on the internalization of values. To the extent that young hackers learn their hacking skills in chatrooms and from websites, they are likely to develop into criminal hackers. If contests can encourage a value-oriented education in hacking, on the other hand, young hackers may be more likely to forswear putting their skills to illicit uses.[187]

participating. On the other hand, to the extent that monitoring contributes to the visibility of hackers' skill, their reputation, and their ability to brag, it may entice some hackers to participate.

184. *See supra* note 91.

185. Note that some hackers may be excluded from the contest if there is reason to believe that they are also engaging in criminal activities. *See supra* Subsection III.B.4.

186. Marc Rogers has attempted to disaggregate "hacking" by categorizing hackers into seven groups: tool kit/newbies (those relying on prewritten software), cyberpunks (vandals with some programming capabilities), internals (disgruntled employees with system access), coders (those familiar with programming techniques and able to write original code), old-guard hackers (with no criminal intent), professional criminals, and cyberterrorists (the most dangerous). Rogers, *supra* note 76, at 9. Drawing on this taxonomy, John Van Beveren traced hacker development and charted their motivations from tool kit/newbies into either cyberpunks or old-guard type hackers. The model tracks how tool kit/newbies develop skill and experience, gathering information from books, magazines, and hacker websites. Unauthorized intrusion committed by tool kit/newbies appears to be a gateway activity that could lead to either malicious or nonmalicious hacking. Van Beveren, *supra* note 151, at 5.

187. The most powerful aspect of preference shaping, and the contests, may be their "second-generation effects"—the fact that a current change in policy will be internalized in future years, shaping actors' beliefs. *See* Katyal, *supra* note 75, at 2444 (noting that current changes in incentive structures will shape how future actors perceive their desires). While preferences in the current generation may be skewed toward counterculture posturing, a generation of hackers raised in an atmosphere where hacking is valued for its social benefits may be more apt to prefer the socially approved game situs for hacking than illegal hacking.

Several "harder" contest features mitigate the possibility that contest participants will move on to more destructive kinds of hacking. The penalty enhancements described in the previous Part are designed to curb hacking outside of the competitions by making it both unattractive and prohibitively costly.[188] As noted above, contests will also allow law enforcement to focus resources on the most deviant kinds of hacking. Another key effect of the contests is that sites themselves will become harder targets after sponsoring contests, reducing the success of illegal hacking efforts. Two computer scientists at Harvard recently argued that organizations that share security information are less attractive to malicious hackers.[189] By sponsoring contests, firms may thus identify themselves as a site that malicious hackers should avoid. Finally, as hacking becomes destigmatized through the contests, more hackers may be willing to help law enforcement track and detect criminally minded hackers.[190] Each of these factors mitigates the problem suggested by the training ground thesis.

Third, criminal law scholars have noted that, because of the substitution effect, punishments for one crime may increase other kinds of crime that are just as serious or perhaps even more dangerous. The relationship between crack cocaine and heroine provides a clear example.[191] While no reliable data on drug use exist, it is likely that the penalty structure for these drugs—the crack to heroin punishment ratio is somewhere between 80:1 to 400:1—would encourage drug dealers and users to substitute heroin for crack to avoid the more severe penalties.[192] Both income and substitution effects are at work here. The income effect predicts that an increase in the price of a good (conceived in terms of either monetary cost or severity of punishment) reduces the real income of a consumer of that good. The substitution effect tempers the income effect of a price increase, however, when the consumer switches to a cheaper good. In some circumstances, such as when heroin is substituted for crack cocaine, the substitute may be more harmful than the targeted activity. Thus, the income and substitution effects, when applied to criminal law, suggest that under some conditions a high price—whether monetary or legal—for one crime may increase the commission of other, perhaps more socially damaging, crimes.[193]

188. *See supra* Part III.

189. Hafner & Biggs, *supra* note 118.

190. *See, e.g.*, TSUTOMU SHIMOMURA, TAKE DOWN (1996) (describing a hacker who helped law enforcement track and capture Kevin Mitnick, a notorious computer criminal); Leslie Walker, *Taking a Whack at Hackers*, WASH. POST, Jan. 13, 2000, at E1 (describing "[a] new breed of security firms" and their practice of hiring "hacker trackers").

191. *See* Katyal, *supra* note 75, at 2402-08 (analyzing crack cocaine and heroin in terms of the substitution effect).

192. *Id.* at 2404-05.

193. *Id.* at 2388.

Applying substitution analysis to the hack-in contest proposal, should we expect hack-in contests to produce an increase in crime? Substitution generally suggests that an increase in the cost of one crime will increase the incidence of a substitute crime that is less expensive. Analogizing from this insight, one might argue that, while the substitution effect will encourage hackers to substitute away from criminal hacking toward hacking in the contests, the income effect may encourage an increase in both activities because a hacker's overall "resources" will go further than before. To address the substitution objection, it will be useful first to clarify the relationship between unauthorized access and other types of crime. Second, having considered both the nature of the increased "resources" a contest participant would have and the relevant characteristics of the contest framework outlined above, we will question whether the income effect has any predictive value in this context.

With respect to the first issue, it is unlikely that hackers engaged in unauthorized access will substitute other types of crime. It bears repeating that the contests do not target profit-motivated computer crime. The elasticity of substitution, the ease with which the demand for one crime may be substituted for the demand for another, is small with respect to unauthorized access because it is a crime with specific payoffs, such as intellectual stimulation and pride, rather than generalizable payoffs, such as money, which can motivate a variety of criminal activity. Moreover, because hackers, particularly those engaged in unauthorized access, have sunk costs in skill development, they are unlikely to engage in other types of crime.[194] Each of these points suggests that those hackers targeted by the contests—hackers engaged in unauthorized access—are unlikely to substitute toward other kinds of crime.

The second part of the objection states that because the cost of the legal substitute—hack-in contests—is cheap, hackers have more "resources" to devote to criminal hacking.[195] With respect to unauthorized access, it is not clear what kinds of "resources" would accrue to a hacker who participates in contests as a result of the income effect. The income effect would neither increase a hacker's available time nor his monetary resources. Skill is the most likely resource a hacker would develop. If skill development lies at the heart of the objection, however, the argument simply reiterates the "sandbox" complaint in different language and is subject to the same response.

Assuming that there would be an independent income effect in this context, the argument is susceptible on its own terms. In order to accurately

194. *See, e.g.*, *id*. at 2442 (noting that "[s]ometimes criminal activity has sunk costs" and that "criminals may not be able to transfer their skills to other areas").

195. The assumption is largely unwarranted. The substitution and income effects come most clearly into play with respect to crimes of consumption or profit-motivated crimes. *Id*. at 2432-33.

assess the income effect's impact, we must consider the mechanism that is built into the contest framework to address this problem. As the cost of "good" hacking in contests decreases, the cost of illegal hacking increases for contest participants due to the penalty enhancements that would apply.[196] Discounting the probability of capture, it is not clear what impact the income effect would have in these circumstances, where a fall in the price of a legal "good" is accompanied by an increase in the price of its illegal substitute. Moreover, the critique fails to consider the extent to which the contest is an appropriate substitute for illegal unauthorized access,[197] and whether, by legitimizing a previously marginalized activity, it may actually improve on the illegal substitute, supplying hackers with a superior "good" at a lower cost. Thus, while the worry about the development of skill "resources" is best stated in the form of the "sandbox" argument, the mechanism by which the substitution and income effects could lead to increased crime has little independent explanatory power with respect to the hack-in contest model.

Fourth, one might argue that bragging rights would be greater for hackers acting outside of the contest framework. While these bragging payoffs may be potentially higher than the reputational gains available through the contests, the risks would also be greater. Since by its nature bragging, unlike the crimes themselves, is easily detectible and traceable, most culprits are discovered because they have bragged.[198] The reallocation of law enforcement resources resulting from the contests would mean that such bragging would receive even greater law enforcement attention. Law enforcement strategy would likely include targeting braggers for violations of substantive law, reinforcing contests as the most important source of prestige in the hacker community. The expected severity of the penalty for braggers would also likely increase, since penalty enhancements would apply to hacking on contest websites and to hacking by former contest participants. Moreover, government could take steps to shame hackers who brag about illegal hacking exploits and are caught, emphasizing the contests as the primary source of hacker prestige.[199] While it is not possible to eliminate the risk that some hackers may seek bragging rights outside of the contest framework, that possibility is less dangerous than it would appear at first glance.

196. *See supra* Subsection III.B.2.

197. This question turns on two issues: (1) the ability to provide the utility obtainable through unauthorized access, namely reputation and intellectual stimulation; and (2) whether there is a strong preference in the hacker community for unauthorized access over contests. If bragging rights are available through the contests and the contests are challenging and frequent, the first requirement should be met. Anecdotal evidence indicates that hackers may actually prefer contests or other legal hacking venues to engaging in illegal activities. *See supra* Subsection III.B.4.

198. *See* Cha & Schwartz, *supra* note 149 (reporting on bragging by hackers).

199. *See supra* note 137 and accompanying text.

Fifth, hacking may be addictive. If so, one might argue that encouraging the activity through privately sponsored contests might lead to increased, compulsive hacking in undesirable instances. Anecdotal evidence indicates that there is some truth to the addiction thesis. In an early trial of the notorious hacker Kevin Mitnick, the judge sentenced him to rehabilitation for his addiction.[200] Also, in the case of *Regina v. Bedworth* in the United Kingdom, the jury acquitted Paul Bedworth of hacking offenses, accepting his defense that an addiction to hacking precluded him from having the requisite intent to be convicted.[201] Concerned about the addictive potential of a variety of Internet activities, Dr. Kimberly Young, a clinical psychologist, has set up the Center for Online Addiction.[202] These developments notwithstanding, the addiction thesis is not altogether noncontroversial. Others have stressed that "[t]he addictive aspects of hacking . . . only partially describe an activity that has an array of intermingled motivations" and have distinguished between intellectual curiosity and compulsion.[203] Even assuming that some hackers are addicted, however, it would seem that offering a harmless substitute is a better solution than leaving them to continue engaging in illegal unauthorized intrusion.[204] The question is whether a hacker's addiction will be fed in a structured, socially beneficial manner, or whether it will be satisfied in some potentially more harmful way. While counseling may be appropriate in the most severe cases, hack-in contests can mitigate much of the social loss associated with addictive hacking. For hack-in contests to provide a safe substitute for addicted hackers, the contests must be frequent so that these hackers do not feel compelled to engage in illegal hacking.

Implicit in the suggestion that hacking may be addictive is the idea that "good" and "bad" hacking are complements, an increase of one promoting an increase of the other. The perceived permeability between the two kinds of hacking, seemingly illustrated at the Black Hat and DEFCON events where security experts and hackers mingle, is misleading. Hackers have long been marginalized and faced with few avenues through which to

200. Paul Feldman, *Prop. 187 Ruling Frustrating for Voters*, L.A. TIMES, Nov. 22, 1995, at A1.

201. *Computer Hackers "Broke into NASA,"* HERALD (Glasgow), May 21, 1993, at 12.

202. *See* Ctr. for Online Addiction, *at* http://www.netaddiction.com (last visited Mar. 4, 2003).

203. TAYLOR, *supra* note 9, at 48.

204. The distinction between *reactions to* and *preconditions for* an addiction is an important one. Efforts to deter hacking through the criminal law, as noted above, have largely failed. To the extent that hacking is compulsive or addictive, these addictive habits preexist hacking contests. Thus, hacking contests constitute a *reaction to* dependence and, as such, they can provide an outlet for compulsive hacking that is not socially harmful. It is also possible that contests will contribute to the creation of new or strengthened addictions in some hackers, resulting in an increase in socially undesirable hacking. As the distinction between socially useful hacking and illegal unauthorized access hardens, however, and contests begin to be sponsored more frequently, this risk should subside.

engage in legitimate hacking.[205] Moreover, this labeling or lumping process, as argued above, can have the unfortunate result of solidifying deviant attitudes.[206] Now that hackers are gaining acceptance in the security community,[207] the boundary between "good" and "bad" hacking appears blurred. The currently unstable boundary is not so much a marker of permeability, however, as an indication that former categories are losing their resonance. As space opens for some kinds of hacking to be considered legitimate, hacking is no longer stigmatized per se, and hackers formerly engaged in illegal hacking shift to activities that are considered socially beneficial. While some "gray-hat" hackers do profess to straddle this boundary,[208] recent developments indicate a shift of attitudes capable of distinguishing between good and bad aspects of hacking that had formerly been homogeneously labeled as illegitimate.[209] Thus, the current lack of clarity appears to be part of the process of reconfiguring boundaries.

Finally, it is possible that a hacker who participated in a contest and uncovered a vulnerability would choose not to reveal it, resulting in greater insecurity rather than target hardening. After the contest, the hacker could compromise the site for any number of purposes—to engage in fraud, theft, or vandalism, or to use the site as a platform from which to engage in such activities. While this would be a serious concern for an independent site

205. TAYLOR, *supra* note 9, at 123 (arguing that the "computer security industry shows a marked reluctance to differentiate between 'responsible hackers' and vandals"); *see also* Katyal, *supra* note 75, at 2398 (recognizing that "stigmatization costs," the ostracization of those who have engaged or who are suspected to have engaged in illegal activity, are an important factor contributing to the perpetuation of criminal activities by certain actors).

206. *See* Katyal, *supra* note 75, at 2444-45, 2457-61 (arguing that stigmatization reduces the cost of future criminal activity, since reputational costs have already accrued, and may lead to the creation of subgroup norms favoring criminality); *supra* note 80 and accompanying text.

207. Amanda C. Kooser, *Hack Away: If Being Hacked Is Inevitable, Wouldn't It Be Better if the Hackers Were on Your Side?*, ENTREPRENEUR, Mar. 1, 2002, at 20 (describing Rent-a-Hacker Inc., a company that draws on hacker knowledge to strengthen customers' computer systems); Susan Moran, *Now Hiring: Hackers*, CHI. TRIB., Apr. 12, 1998, § 6, at 1 (noting the increasing frequency with which hackers are hired to help toughen Internet security); Dequendre Neeley, *Hire Thine Enemy? (How To Prevent Computer Attacks)*, SECURITY MGMT., Sept. 1, 1999, 1999 WL 14496643 (noting the growing trend to hire "underground hackers and system crackers either as consultants or regular staff to conduct penetration tests on their networks"); Bob Violino, *Hackers for Hire*, INFORMATIONWEEK, June 21, 1993, LEXIS, Nexis Library, InformationWeek File (quoting Dorothy Denning as saying that "[i]f you really want to find out if your system is protected against hackers, you must have hackers beat away at it").

208. Gottlieb, *supra* note 88, at 36 (describing the hacker group L0pht as "gray-hat," a morally ambiguous position, for its willingness to help government and enhance Internet security as well as to advise malicious hackers). In addition to gray-hats, hackers are typically characterized as black-hat—those who hack maliciously—and white-hat—those who hack legitimately, including security staff and researchers. Jude Thaddeus, *The Confessions of a White Hat Hacker*, COMPUTERWORLD, Dec. 4, 2000, *at* http://www.computerworld.com/securitytopics/security/story/0,10801,54616,00.html.

209. Helen D'Antoni, *Hacker Hires Don't Interest Most Businesses*, INFORMATIONWEEK, Oct. 22, 2001, *at* http://www.informationweek.com/story/IWK20011019S0002 (noting that, while "the idea of hiring a hacker remains inconceivable for many business-technology professionals," half of the polled employers expressed a willingness to hire a hacker as a consultant).

sponsoring a contest without government support, it is much less problematic in the framework laid out above. Both the penalty enhancements, which would apply to contest participants, and the honeypot monitoring suggestion, which could record each participant's activities for later review, address this problem. Rather than actually monitoring participants' activities, contest sponsors could equip their sites with an "early warning" alarm system such that no contest participant could breach security without the sponsors being notified. To the extent that formal monitoring, or even the less intricate alarm system, is impractical due either to cost or hacker reluctance to participate in such contests, law enforcement could agree to prioritize contest sponsors who have been hacked. A menu of options is thus available to minimize the possibility that sponsors would be victimized by contest participants.

The challenges to hack-in contests assessed above do not undermine the proposal's strength. If implemented so as to account for hackers' motivations, reputations, and competitive spirits as well as their desire for social legitimacy, contests could play a powerful preference-shaping role in the hacker community. Contests must be integrated with criminal sanctions, however. Preference shaping through criminal law alone will be relatively ineffective. Thus, shaping preferences by creating incentives to induce positive behavior may nurture hacker ethics that value law-abiding behavior. Over the long term, contests may help develop hacking norms that encourage obeying the law. These contests may particularly impress young people—those most prone to vandalism—who have not yet become socialized within a particular hacking subculture. If a young hacker thinks others are obeying the law and getting their biggest hacking thrills from competing in organized games, he may choose the same route.[210] The contests' objective is to cultivate strong preferences among hackers for law-abiding behavior. While government must reinforce this process, savvy marketing that sells the idea to hackers is an essential part of the approach.

CONCLUSION

Many of the policies used to deter computer crime have proved ineffective. Despite criminal penalties and regulation through code itself, hackers continue to intrude into private networks with impunity. At the same time, the social response to computer crime remains embryonic. Popular attitudes are still largely plastic. In this context, it is important to

210. Akers et al., *supra* note 100, at 638 (emphasizing the influence of peer groups on behavior); Dan M. Kahan, *Signaling or Reciprocating? A Response to Eric Posner's* Law and Social Norms, 36 U. RICH. L. REV. 367, 368-69 (2002) (arguing that, as moral and emotional reciprocators, people conform their actions and attitudes to reflect what they believe to be the behavior of others around them).

begin shaping attitudes with nonlegal tools. Contests, like those proposed in this Note, may play a role in turning normal hacking behavior away from unwarranted intrusions.

The contest seeks to interweave the moral message of the criminal law with the hacker's culture of openness on the web. It balances the benefits of decriminalization with the need to maintain a clear prohibition on criminal hacking, and it is tailored to the culture of the community it is meant to affect. The contest provides the benefit of having "eyes on the street" without giving hackers carte blanche to invade private networks or individually price their conduct. With many hacking tools already available for download from the web, hacking has been democratized and may well be on the road to normalization. It is important to experiment with new policies that might begin to shape preferences effectively. By reinforcing criminal sanctions and positive social meanings through positive incentives, a system of structured contests may be an important means of nurturing socially beneficial hacking norms that are largely self-enforcing.