Journal of Criminal Law and Criminology

Volume 97
Issue 2 *Winter*

Article 6

Winter 2007

Virtual Neighborhood Watch: Open Source Software and Community Policing against Cybercrime

Benjamin R. Jones

0091-4169/07/9702-0601
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY
Vol. 97, No. 2
Printed in U.S.A.

COMMENT: VIRTUAL NEIGHBORHOOD WATCH: OPEN SOURCE SOFTWARE AND COMMUNITY POLICING AGAINST CYBERCRIME

BENJAMIN R. JONES*

Cybercrime—crime committed through the use of a computer—is a real and growing problem that costs governments, businesses, and individual computer users millions of dollars annually and that facilitates many of the same crimes committed in realspace, such as identity theft and the trafficking of child pornography, only on a larger scale. However, the current strategies deployed by law enforcement to combat cybercrime have proven ineffective. Borne out of traditional notions of criminal behavior, these strategies and tactics are often ill-suited to prevent or punish cybercrime, which often defies the traditional notions of criminal behavior bounded by the corporeal world such as scale and proximity. This Comment argues that a more effective methodology in the fight against cybercrime is to develop a model of community policing, in which the power to deter and prevent cybercrime is divested into the hands of individual computer users. One such strategy for achieving effective community policing against cybercrime is through the increased use of open-source software, software in which users are given access to the underlying source code and may make modifications to that source code in order to ameliorate vulnerabilities that may enable cybercrime. This Comment looks at the development of traditional community policing strategies and argues that the increased use of open source software—spurned by greater involvement by government and corporations—may be a more effective technique in the fight against cybercrime.

I. INTRODUCTION

One of the few constants of the Internet age is the recognition that technology and the law are not always the best dance partners.[1] From the

* J.D. 2007, Northwestern University School of Law.

[1] *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS 5-6 (2002).

effect of Internet file-sharing technologies on copyright law[2] to the impact of e-commerce on notions of jurisdiction,[3] there is often a fundamental disconnect between laws written to govern the corporeal world of "realspace" (the tangible, real world, as distinguished from the virtual world of cyberspace) and technological advances, which enable the almost instantaneous flow of information across the globe. From the time of the framing of the Constitution to the present, the development of new technologies has created challenges and opportunities beyond the conceptual scope of legislators and courts. Modern policymakers have struggled to close the gap between the technological world and the legal world.[4]

Perhaps the most fundamental change wrought by the development of the Internet is the way in which information now moves. A user sitting in front of a computer connected to the Internet can access a virtually boundless stream of information—from the price of gold on the Tokyo currency exchange to the home movies of a Muscovite, back from a first vacation in Las Vegas—moving at nearly the speed of light. These changes in the flow of information have impacted almost every facet of society—from commerce to communication to government, reshaping many of the ways in which we interact.

Not surprisingly, the impact of this revolution in the flow of information extends to the criminal world as well. Criminals and potential criminals have seized upon the power of the Internet to enable the commission of a host of crimes—from the sale of illegal drugs to the trafficking of child pornography—and to expand the criminal enterprise into the commission of an entirely new breed of crime, possible only in the virtual world of computer technology.[5] A quick scan of newspaper headlines over the past five years reveals the breadth and impact of cybercrime.[6] Indeed, the spread of cybercrime has reshaped the modern

---

[2] *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 918 (2005) (holding that peer-to-peer file sharing service did not fall within the protection of the fair use exception to the copyright statute).

[3] *See* Gator.com, Corp. v. L.L. Bean, Inc., 341 F.3d 1072, 1081-82 (9th Cir. 2003) (holding that an e-commerce website directed sufficient activity at customers in California to establish general jurisdiction over the company in California, despite the fact that the company did not maintain a physical presence in California).

[4] *See* LESSIG, *supra* note 1.

[5] *See* Neal K. Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1004 (2001) [hereinafter Katyal, *Criminal Law in Cyberspace*].

[6] *See, e.g.*, Chris Nuttall, *Melissa Virus Goes Global*, BBC NEWS, Mar. 30, 1999, http://news.bbc.co.uk/1/hi/sci/tech/307162.stm; John Schwartz, *No Love for Computer Bugs*, WASH. POST, July 5, 2000, at A1.

lexicon to include new definitions for words such as "identity theft," "worm," and "Trojan Horse."[7]

Like the relationship between law and technology, the strategies and tactics of modern law enforcement also lag in responding to the new challenges posed by cybercrime.[8] Importantly, the reactive model of law enforcement—developed over centuries in response to traditional, realspace crime—is ill-equipped to combat the challenge of cybercrime, unbounded by the constraints of the physical world.[9] As one commentator notes, "Like the common law, the traditional model of law enforcement is a compilation of past practices that have been deemed effective in dealing with the phenomena it confronts. The model's general strategy, the reactive approach, is one that has been in use since antiquity."[10]

This reactive approach, focused on identifying a crime, apprehending the perpetrator, and meting out some punishment through the justice system, emerged as a response to crimes in the real world, constrained by the simple laws of physics. Important among those limits are notions of proximity and scale.[11] For most crimes, the perpetrator must actually be physically proximate to his victim.[12] A pickpocket in nineteenth century London could not remove the wallet of a gentleman across town; he would have to get within close proximity of his unwitting victim, risking detection or failure. The scale of most crimes was also one-to-one; a single perpetrator targeted a single victim before he could move onto the next crime.[13] That same pickpocket could not simultaneously remove the wallets of a thousand Londoners. The limits of proximity and scope made it relatively easy to identify the perpetrator and the specific instances of

---

[7] Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1023-27.

[8] Susan W. Brenner, *Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 RUTGERS COMPUTER & TECH. L.J. 1 (2004) [hereinafter Brenner, *Law Enforcement*]; Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 8 U. PITT. J. TECH. L. & POL'Y 1 (2005) [hereinafter, Brenner, *Product Liability*]; Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465 (1997); Katyal, *Criminal Law in Cyberspace*, *supra* note 5.

[9] *See generally* Brenner, *Law Enforcement*, *supra* note 8; Brenner, *Product Liability*, *supra* note 8 (Brenner, like other scholars, notes the impact of computer technology on both the commission of crimes and attempts by police to prevent and prosecute those crimes. Cybercrime and cybercriminals are simply not bounded by the physical constraints of realspace that limit the reach and methodology of certain criminal acts; as described, *infra*, a pickpocket in nineteenth century London could not pick the pockets of one thousand people around the city in one act—the laws of physics prevent it.).

[10] Brenner, *Law Enforcement*, *supra* note 8, at 22.

[11] *See id.*

[12] *See id.*

[13] *See id.*

crime, and law enforcement officers could focus on capturing the individual perpetrator.[14]

It is increasingly clear, however, that those same constraints of proximity and scale do not bind criminals operating in the virtual world of cyberspace.[15] The Internet, which connects millions of computers (and computer users), allows criminals to commit crimes anonymously against victims thousands of miles away.[16] Importantly as well, those crimes are far from one-to-one in scale.[17] Our old friend the pickpocket, operating in twenty-first century London, could unleash a "worm" that affects computers around the world and causes millions of dollars in damage or that gains access to the computer system of a bank in Seattle and loots the accounts of hundreds of customers at the same time. The fundamental difference between cybercrime and crime in realspace means that the current strategies designed to combat realspace crime, particularly those predicated upon the reactive approach, are ill suited to combat the increasing problem of cybercrime.

This Comment explores the notion that current strategies designed to prevent and punish cybercrimes are ineffective and argues that the community policing model may provide an alternative for more effectively deterring and punishing cybercrimes. Section II provides an introduction to the growing problem of cybercrime and its various forms.[18] Section III illustrates how current strategies focused on punishing perpetrators of cybercrime are ineffective.[19] Section IV describes the community policing model and demonstrates how this model can be applied to create effective deterrents to cybercrime.[20] Finally, Section V argues that the increased use of open source software—especially in the operating system and Internet browser markets—is an important tool in making the community policing model a success.[21]

II. WHAT IS CYBERCRIME?

At the outset, it is helpful to describe exactly what is meant by the term cybercrime, as it is a label applied to acts ranging from the propagation of

---

[14] *See* Brenner, *Product Liability*, *supra* note 8, at 14.

[15] Brenner, *Law Enforcement*, *supra* note 8, at 25-30.

[16] *See generally id.*

[17] *See id.*

[18] *See infra* Section II.

[19] *See infra* Section III.

[20] *See infra* Section IV.

[21] *See infra* Section V.

computer viruses to cyberstalking.[22] At the broadest level, cybercrime can be described as any crime committed through the use of a computer or computer technology, but a more specific taxonomy helps classify the different types of offenses.[23] Although specific definitions will vary, cybercrimes can be placed in four broad categories—unauthorized access to computer programs and files, unauthorized disruption, theft of identity, and carrying out of traditional offenses, such as distribution of child pornography, using a computer.[24]

A. UNAUTHORIZED ACCESS

Unauthorized access occurs whenever "an actor achieves entry into a target's files or programs without permission."[25] This access can be achieved either remotely—by gaining access to the target computer from another computer connected over a network—or physically, by using the target computer.[26] Interestingly, the crime of unauthorized access—however it is defined under federal or state criminal codes—is the unique crime of invading another's private workspace, in and of itself.[27] Malicious acts such as "causing harm to the files or programs or using the data improperly" are classified as separate crimes of their own.[28]

The targets of unauthorized access are most commonly the government, corporations, or private individuals.[29] The government is an obvious target because its vast computer files contain a myriad of sensitive information, ranging from the Department of Defense plans for military contingencies to law enforcement information on individuals and criminal

---

[22] *See* Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1020-38.

[23] Federal law provides an expansive definition of cybercrime, prohibiting certain forms of unauthorized access and actions that exceed the scope of authorized access to any computer used across state lines. *See* 18 U.S.C. § 1030 (2000). In 1994, Congress modified the statute so that the requisite mens rea was "intentional, knowing, and reckless"; that amendment was further changed in 1996 to impose strict liability on alleged perpetrators of cybercrime. *See* S. REP. NO. 104-357, at 10-11 (1996); *see also* United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996) (holding that the statute does not require proof that the defendant had the intention to damage computer files). In addition, all fifty states have promulgated laws criminalizing cybercrimes. *See, e.g.*, CAL. PENAL CODE §§ 502, 502.01 (2006); 720 ILL. COMP. STAT. 5/16D-1-5/16D-7 (2006); N.Y. PENAL LAW §§ 156.00-.50 (McKinney 2006).

[24] *See* Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1020-38.

[25] *Id.* at 1021.

[26] *See id.*

[27] *See id.*

[28] *Id.*

[29] *Id.*

organizations.[30] Access to a corporation's computers places at risk information ranging from proprietary business documents and trade secrets to private customer information like credit card account numbers and social security numbers.[31] The unauthorized use of personal computers may reveal the same personal financial information as described above, but also risks harms to individual privacy.[32] Computer files may contain private information "as personal as love letters, as banal as grocery lists, or as tragic as unfinished drafts of law review articles," the loss of which creates a feeling of lost privacy in addition to any quantifiable economic harm.[33]

B. UNAUTHORIZED DISRUPTION

Unauthorized disruption, by comparison, occurs when an individual interferes with the operation of a computer system, whether by gaining unauthorized access or through some other means.[34] Such acts are at "the heart of what most people consider cybercrime."[35] These crimes occur when an actor—human or machine—interferes with computer hardware or software, without permission.[36] The different types of authorized disruption attacks—including viruses, worms, and Trojan horses—are now a familiar part of the lexicon, but again it is helpful to describe the unique features of each.[37]

1. Viruses

In its simplest form, "[a] virus is a program that modifies other computer programs."[38] The modifications ensure that the healthy computer will replicate the virus.[39] Once the now-infected computer is connected to another computer—via the Internet, a direct computer-to-computer connection, or a shared storage disk—the virus can be transferred onto the new computer.[40] Interestingly, viruses are not, in and of themselves,

---

[30] *Id.* As Katyal points out, "The specter of a curious computer geek who gains access to sensitive computers [à la] the 1983 film 'War Games' is not fanciful, as such attacks have occurred successfully on numerous occasions." *Id.*

[31] *Id.* at 1022.

[32] *Id.*

[33] *Id.*

[34] *Id.* at 1023.

[35] *Id.*

[36] *Id.*

[37] *See id.*

[38] *Id.*

[39] *Id.*

[40] *Id.* at 1023-24.

harmful.[41] Their harmful nature depends upon the additional elements, beyond the instructions for self-replication, written into their code.[42] Indeed, there are some viruses which have a benign or merely annoying effect on the computers they infect.[43] Others, however, have caused widespread damage.[44]

2. Worms

A worm is a stand-alone program that is able to replicate itself over a network without any action by the user, unlike a virus, which requires some human action, such as downloading an infected file or placing an infected disk in the computer.[45] Like viruses, the destructive nature of worm programs depends on the additional instructions inserted into the program code beyond the basic instructions for replication.[46] Perhaps the most noteworthy worm is the ILoveYou bug, which infected over a million computers and spread nine times faster than the "Melissa" virus.[47] The infection caused major corporations such as Ford Motor Company and AT&T to shut down their e-mail systems, resulting in lost time and productivity, and also reached the computer systems of government agencies including the Department of Defense, the Central Intelligence Agency, and NASA.[48]

---

[41] *Id.* at 1024.

[42] *Id.*

[43] Kim Zetter, *How a Computer Virus Works*, CNN.COM, Oct. 23, 2000, http://archives.cnn.com/2000/TECH/computing/10/23/virus.works.idg/.

[44] Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1024. A prominent example is the "Melissa" virus, which became public in March 1999. The virus infected its first victim through the alt.sex newsgroup and within days had spread to over a hundred of the Fortune 1000 companies. *Id.* The virus propagated by sending an e-mail, purportedly from the user of the infected computer, containing a Microsoft Word attachment to fifty addresses in the infected computer's electronic address book with the subject line "Important Message from . . . ." Mary Foley & Lisa Bowman, *Melissa Virus Swamps Corporate E-mail*, ZDNET NEWS, Mar. 26, 1999, http://news.zdnet.com/2100-9595_22-514149.html?legacy=zdnn. When a recipient opened the attached document, the virus infected her computer, triggering the same process. *Id.* The virus eventually caused over $80 million in damage. Eric Luening, *Smith Pleads Guilty to Melissa Virus Charges*, NEWS.COM, Dec. 9, 1999, http://news.com.com/2100-1023-234181.html?legacy=cnet. David Smith, a computer programmer from New Jersey, eventually pleaded guilty to state and federal charges for creating and spreading the virus. *Id.*

[45] Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1024.

[46] *See id.*

[47] *Id.* at 1024-25; *see supra* note 44 for a description of the Melissa virus.

[48] Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1025.

3. Trojan Horses

A Trojan horse is a program that appears to perform some useful function, but which also may contain hidden malicious code.[49] The Trojan horse may act as a delivery vehicle for a virus or worm or permit unauthorized access by another.[50] Often, the Trojan horse program will contain spying software or "backdoor" functions that allow a remote user to gain information about the computer or to actually control the computer via the network, creating a "zombie computer."[51]

4. Distributed Denial of Service Attacks

A final type of unauthorized disruption is known as a Distributed Denial of Service (DDoS) attack.[52] These attacks overwhelm websites with network traffic and disrupt their ability to communicate with legitimate users.[53] A DDoS attack begins when:

> [A]n individual obtains unauthorized access to a computer system and places software code on it that renders that system a "Master." The individual also breaks into other networks to place code that turns those systems into agents (known as "zombies" or "slaves"). . . . The Masters are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents. After receiving this information, the agents make repeated requests to connect with the attack's ultimate target, typically using a fictitious or "spoofed" [Internet Protocol] address, so that the recipient of the request cannot learn its true source. Acting in unison, the agents generate a high volume of traffic from several sources. . . . [T]he destination computer becomes overwhelmed . . . . [and] loses all or most of its ability to serve legitimate customers . . . .[54]

DDoS attacks can have a tremendous impact on the flooded target computers, resulting in millions of dollars in lost productivity.[55]

---

[49] *Id.* at 1026.

[50] *Id.*

[51] Trojan Horse Primer, http://windowsecurity.com/articles/Trojan_Horse_Primer.html (last visited Apr. 21, 2007).

[52] *See* Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1026.

[53] *Id.*

[54] *Id.* at 1026-27.

[55] *See id.* at 1027. For example, in 2000, a fifteen-year-old Canadian youth known by the pseudonym "MafiaBoy" allegedly authored a DDoS attack directed at popular Internet sites such as Yahoo!, Amazon.com, CNN.com, and others. *Id.* The attack illustrated the potential vulnerability of Internet business and commerce to cybercrime and contributed, in part, to a 258.44 point drop in the Dow Jones Industrial Average. *See id.* Law enforcement officials were unable to track down the original source of the attack and only learned of the perpetrator after he bragged about the attack in Internet chat rooms. *Id.*

C. IDENTITY THEFT

A third category of cybercrime is identity theft. In its most familiar form, identity theft occurs when an individual—via unauthorized access to digital information—steals the personal information of another, such as the victim's credit card numbers or social security number.[56] Now able to disguise himself as the target individual, the criminal can access the individual's bank accounts, make purchases using the stolen credit card numbers, obtain credit cards in the victim's name, or commit other malicious acts.[57]

There are also other forms of identity theft via computer that do not have a clear realspace analog because they involve the unique properties of computer systems, particularly those linked over the Internet.[58] "Cross-site scripting" occurs when malicious code is inserted into a website, forcing the website to send out information not authorized by its owners.[59] "Page-jacking" involves the reprogramming of an Internet address to take the unwitting user to an alternate site.[60] If a user clicks on a GMC Truck ad atop the ESPN.com website and is instead redirected to an Internet gambling website, the page has been "jacked." Finally, "IP spoofing" occurs when a perpetrator uses software to disguise his Internet Protocol (IP) address to match that of a "trusted" user and is able to gain unauthorized access to a secured computer or website.[61] A criminal with IP spoofing software could mimic the IP address of a corporate employee's home computer to gain remote access to the corporation's computer systems.

D. USE OF COMPUTERS TO CARRY OUT TRADITIONAL CRIMES

A final broad category is the use of computers to carry out traditional criminal offenses. These offenses can range from the distribution of child pornography to the sale of illegal firearms to so-called cyberstalking.[62] While the nature of these offenses does not differ merely because of the use of computer technology, "[e]ach reveals the advantages, from the criminals'

---

[56] *See* Identity Theft and Fraud, http://www.usdoj.gov/criminal/fraud/idtheft.html (last visited Apr. 21, 2007).

[57] *Id.*

[58] *See* Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1027.

[59] *Id.*

[60] *Id.* at 1028.

[61] *Id.*

[62] *Id.*

perspective, of cybercrime—widespread, quick distribution, and cost minimization."[63]

In short, the range of cybercrime is quite broad. The different categories, however, are neither co-extensive nor mutually exclusive; a cybercriminal may choose to carry out only a DDoS attack or gain unauthorized access to a computer network in order to plant a virus and steal the identities of network users. Each of these different types of crime has the power to cause tremendous damage, whether it is economic loss or more intangible harms, such as in the case of the sale of child pornography or the unauthorized access of personal data.

III. WHY CURRENT STRATEGIES ARE INEFFECTIVE

Each of the different types of cybercrimes share one salient feature—the use of computer technology. This technology fundamentally alters the nature of cybercrimes from those committed in the real, corporeal world. Crimes committed in realspace without the use of technology—from murder to pickpocketing—share two significant characteristics: proximity and scale.[64]

A. PROXIMITY

The first of those common elements is proximity.[65] Given the constraints imposed by space and time, a perpetrator of realspace crime must actually be physically proximate to the victim.[66] Of course, there are examples of realspace crime that do not require the perpetrator to be near his victim—for example, securities fraud or the sending of poison through the mail. However, the vast majority of realspace crimes require such proximity.[67] In turn, the notion of proximity has created a presumed dynamic in the model of traditional law enforcement—"victim-perpetrator presence in the same general locale; victim-perpetrator proximity and consequent victimization; perpetrator efforts to flee the crime scene and otherwise evade apprehension; investigation; identification; and apprehension of the perpetrator."[68] Even as modern cities have moved beyond the parochial world where victims and perpetrators tended to live in

---

[63] *Id.*

[64] Brenner, *Law Enforcement*, *supra* note 8, at 3-4.

[65] *See id.* at 3.

[66] *Id.* Indeed, "[p]erhaps the most fundamental characteristic of real-world crime is that the perpetrator and the victim are physically proximate to each other at the time the offense is committed or attempted." *Id.*

[67] *Id.*

[68] Brenner, *Product Liability*, *supra* note 8, at 11.

the same small communities, law enforcement still relies heavily on the spatial limitations of crime.[69] Importantly, "the real-world model still assumes that the investigation of a crime should focus on the physical scene of the crime."[70]

Unlike crime in realspace, however, cybercrime does not require any degree of proximity between the attacker and victim—"[i]t can be committed by someone who is located anywhere in the world against a victim who is in another city, another state, another country."[71] The blessing of the Internet—the simultaneous connection of computer users all over the world—is also a curse when viewed through the lens of cybercrime. An attacker merely needs a computer connected to the Internet in order to gain access to millions of other computers.[72] Having gained that access, he can inflict harm upon others—either directly upon their computer or by accessing information that will allow him to commit future crimes.[73]

The physical separation between attacker and victim also has important consequences for the investigation of cybercrimes. In a virtual world comprised of ones and zeroes transmitted over cables and wires, there is often no "crime scene" for investigators to comb for clues.[74] And, where there is such a crime scene, it can be found in hundreds, if not thousands, of computers and servers owned by corporations and individuals around the world.[75]

Two important advantages conferred upon cybercriminals by the use of computer technology further erode the notion of proximity—anonymity and encryption.[76] As Katyal points out, "Computers . . . confer massive efficiencies on the criminal by hiding the perpetrator's identity and covering data streams."[77] Perpetrators of cybercrime are often identified only by a pseudonymous e-mail address, linked to an IP address, which appears as a seemingly random string of numbers.[78] Without the cooperation of the Internet service provider that maintains the e-mail address, there is almost no way to connect the e-mail pseudonym with the realspace identity and location of the attacker.[79] Moreover, a host of technologies exist that allow

---

[69] *Id.* at 12.

[70] *Id.*

[71] Brenner, *Law Enforcement*, *supra* note 8, at 25-26.

[72] Brenner, *Product Liability*, *supra* note 8, at 14.

[73] *Id.*

[74] Brenner, *Law Enforcement*, *supra* note 8, at 30.

[75] *Id.*

[76] *See* Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1047.

[77] *Id.*

[78] *Id.*

[79] *Id.*

users to mask their true identity, leaving them essentially invisible to detection over the Internet.[80] This anonymity further insulates the criminal from his victim, and shields the criminal from law enforcement authorities responding to an attack.[81] Such anonymity confers a great advantage upon computer criminals as "[e]ven masked or otherwise disguised criminals in realspace may unwittingly indicate their height, race, voice, and now their DNA."[82]

Further adding to the anonymity conferred on computer criminals is the use of encryption technologies.[83] Encryption involves the use of algorithms or other mathematical formulas to encode data into a pattern that is indecipherable except to those who have the password or key to decipher it.[84] While methods for encoding messages predate the computer by millennia,[85] "computers have for the first time put encryption into broad use."[86] From the perspective of criminal law, encryption is uniquely "Janus-faced"—it can be used both by criminals to mask their true identity and to render communications unreadable by law enforcement authorities, but it also can be employed to prevent cybercrimes by protecting confidential data and communications from unauthorized access.[87] The debate over the benign and malign effects of encryption technology could fill volumes far longer than this Comment. Yet the fact remains that such technologies can be employed by cybercriminals both to mask their own identity and to communicate beyond the prying eyes and ears of law enforcement officials.[88]

---

[80] *Id.* at 1048-49.

[81] *Id.* at 1047-48.

[82] *Id.* at 1047.

[83] *See id.* at 1048.

[84] *Id.*

[85] *See, e.g.*, Vicky Ku, Note, *A Critique of the Digital Millennium Copyright Act's Exemption on Encryption Research: Is the Exemption too Narrow?*, 7 YALE J.L. & TECH. 465, 470 (2005), *available at* http://research.yale.edu/lawmeme/yjolt/modules.php?name=News&file=categories&op=newindex&catid=10.

[86] Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1048.

[87] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 4 (1999).

[88] *See generally* STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST: CRYPTOGRAPHY, GOVERNMENTS, AND ELECTRONIC COMMERCE (1998); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); Edward J. Radlo, *U.S. Encryption Export Regulations Enter the Twenty-First Century*, COMPUTER LAW., June 2000, at 31.

B. SCALE

The second characteristic of traditional crime is its scale.[89] Real-world crime tends to consist of a single event with one perpetrator and one victim:

> The "crime" commences when the victimization of the target is begun and ends when it has concluded; during the event the perpetrator focuses all of his or her attention on the consummation of that "crime." When the "crime" is complete, the perpetrator is free to move to another victim and another "crime."[90]

The one-to-one nature of real-world crime is a generality, more than an absolute.[91] One can think of many examples—especially with the advent of organized crime and gang violence—where multiple perpetrators commit the same crime against one victim.[92] However, the opposite—the perpetration of crimes against many individuals by one criminal—is rare without the use of technology.[93] There are certain criminal acts—ranging from terrorism and genocide to corporate fraud and environmental pollution—that defy this traditional notion of scale and involve the commission of a single criminal act that impacts a large number of victims. However, as in the case of realspace crimes that do not require proximity, such crimes represent only a small number of the total crimes committed in realspace, and—perhaps more importantly—they have not had a profound effect on the development of traditional law enforcement techniques.

Cybercrime reverses the traditional notion of the one-to-one scale of crime in realspace.[94] Particularly, the use of technology acts as a force multiplier that "vastly increases the number of 'crimes' an individual can commit and the speed with which she can do so."[95] The cumulative scale of cybercrime is particularly troublesome for traditional law enforcement efforts; police are accustomed to responding to and investigating single-victim, single-perpetrator crimes.[96] Cybercrime, by contrast, is committed

---

[89] Brenner, *Law Enforcement*, *supra* note 8, at 4.

[90] *Id.*

[91] *Id.* at 5.

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.* at 28; *see also* PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET (2000), *available at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#CHALLENGES ("The potential to reach vast audiences easily means that the scale of unlawful conduct involving the use of the Internet is often much wider than the same conduct in the offline world. To borrow a military analogy, use of the Internet can be a 'force multiplier.'") (emphasis omitted).

[96] Brenner, *Law Enforcement*, *supra* note 8, at 28.

on a far greater scale and represents an entirely new set of offenses that must be investigated along with the spate of traditional crimes.[97]

Cybercrime, unlike terrestrial crime, is also automated; a criminal can set in motion a series of repeated attacks by uploading a single virus or worm or initiating a single DDoS attack.[98] Automation "allows a perpetrator to commit thousands of crimes quickly and with little effort, making one-to-many victimization a realistic default assumption for cybercrime."[99] The ILoveYou worm provides a staggering example of how widely and quickly one act of cybercrime can spread among millions of computer users across the world.[100] And, the speed and reach of cybercrime can only be expected to increase in lockstep with the increase in the number of computer users, particularly those who rely on computers connected to the Internet.

The automated nature of cybercrime is particularly troubling for law enforcement officials.[101] After the commission of a real-world crime, officers react by investigating and, hopefully, identifying and apprehending the perpetrator.[102] Cybercrime frustrates this traditional response.[103] Though cybercrime—like real-world crime—is carried out by only a relatively small fraction of the population, "this relatively small group can commit crimes on a scale far surpassing what is possible in the real-world, where one-to-one victimization and serial crimes are the norm. As a result, the absolute scale of cybercrime, in terms of incidence of discrete crimes, exponentially exceeds that of real-world crime."[104]

The traditional notion of crime control is, by and large, monolithic. It has emerged over the centuries as a response to crimes that, except for a few examples at the margins, share two salient characteristics: proximity and scope. Cybercrime, however, turns the notions of both proximity and scope upside down as computer criminals can take advantage of technology to perpetrate crimes against victims from across great distances and against large numbers of victims in a single act. The differences in the fundamental aspects of cybercrime demand a change in the strategies designed to combat that crime if we are to be successful in fighting such crime in the future.

---

[97] *Id.* at 29.

[98] Brenner, *Product Liability*, *supra* note 8, at 14.

[99] *Id.* at 14-15.

[100] Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1024-25.

[101] Brenner, *Product Liability*, *supra* note 8, at 15.

[102] *Id.*

[103] *Id.*

[104] *Id.*

IV. THE COMMUNITY POLICING MODEL

Given the shortcomings of the traditional law enforcement model to combat cybercrime, we must look for alternatives. As Brenner succinctly recommends, "We do need a new approach, particularly for cybercrime, because the traditional model is not . . . a workable solution for online crime."[105] Reworking the law enforcement model to stem the tide of cybercrime must begin with our understandings of the fundamentally different nature of cybercrime and the shortcomings of the reactive nature of traditional police work. This Comment suggests that the best way to combat the problem of cybercrime is to shift the focus from reacting to cybercrimes ex post, to preventing those crimes ex ante, before they occur. As this Comment suggests, one creative approach to achieving such prevention is to decentralize the responsibility for policing the Internet among the community of computer users, enabling changes at the code level that create effective deterrents against the commission of cybercrime.

This notion of community policing is neither new nor unique to the virtual space of the Internet. The concept of community policing arose in the 1970s and 1980s as scholars and policymakers looked to devise new solutions to the problems of crime and poverty plaguing America's inner cities.[106] A growing consensus realized that relationships between police officers and citizens in these communities had become untenable.[107] Many police departments and individual officers on the streets had embraced the so-called "warrior model," in which they saw themselves as doing battle with an ever-present adversary among the citizens in the community.[108] This notion, in turn, led officers to believe that the public saw them in an equally hostile fashion.[109] At the same time, criminological research began to reveal the inadequacy of police tactics of the day, which led to increasing

---

[105] Brenner, *Law Enforcement*, *supra* note 8, at 41.

[106] *See* James Forman, Jr., *Community Policing and Youth as Assets*, 95 J. CRIM. L. & CRIMINOLOGY 1, 4-5 (2004).

[107] *See, e.g.*, Jack R. Greene, *"Community Policing and Organization Change," in* COMMUNITY POLICING: CAN IT WORK? 30, 35 (2004).

[108] *See* Forman, *supra* note 106, at 4-5; *see also* GEORGE L. KELLING & CATHERINE M. COLES, FIXING BROKEN WINDOWS 82-85 (1996).

[109] For example, a study by William Westley in 1970 indicated that 73% of police officers felt that the public was "against the police" or "hates the police." Forman, *supra* note 106, at 5 (quoting WILLIAM WESTLEY, VIOLENCE AND THE POLICE: A SOCIOLOGICAL STUDY OF LAW, CUSTOM, AND MORALITY 93 (1970)). Only 13% of officers believed that "some are for us, some against us," and 12% believed that citizens "like[d] the police." *Id.*; *see also* JAMES Q. WILSON, THINKING ABOUT CRIME 117 (rev. ed. 1983) ("The view of many big city police officers seems to confirm the 'war' theory of police-community relations. Data gathered at least as far back as 1960 suggest that most big-city officers see the citizenry as at best uncooperative, at worst hostile.").

the number of patrol officers, random saturation patrols, and rapid response to 911 calls.[110] In sum, "the research undermined many of policing's core assumptions, thereby creating an opening for reformers to offer new approaches."[111]

Central to the paradigm shift away from the warrior model was the recognition that, despite police perceptions about citizens' hostilities, inner-city residents actually held a favorable impression of the police.[112] "Even more profoundly, it meant understanding that even those who were critical did not want less policing—they generally wanted more, and better, protection."[113] This understanding of community support for the police was buttressed by a notion that even high crime communities are composed of a majority of law-abiding citizens.[114] "Community policing was built upon the import of these findings, and its challenge was to replace the warrior model with one premised on the notion that the police and the community could become co-producers of public safety, rather than hostile antagonists."[115]

The community policing model not only sought to improve the relationship between citizens and police officers, but also to give citizens an active role in "policing" their communities:

> At its core, community policing is not a set of tactics, but instead is an organizational strategy for running a [police] department. In its most promising form, this strategy has two essential elements. First, it requires that citizens, at the neighborhood level, meet regularly with police to jointly define neighborhood crime problems and set police priorities. . . . The second critical element is that citizens, again at the local level, take responsibility for helping to address the problems that they have identified.[116]

This set of tactics includes having officers physically walk through neighborhoods, rather than patrolling in cars, and hosting community building events such as prayer vigils and midnight basketball leagues. But,

---

[110] Forman, *supra* note 106, at 5.

[111] *Id.*

[112] *Id.*; *see also* Tracey L. Meares, *Praying for Community Policing*, 90 CAL. L. REV. 1593, 1599 (2002) ("It is . . . clear, however, that community-policing strategies constitute a rejection of policing policies that became popular in the sixties and seventies emphasizing 'the three Rs: rapid response, random patrols, and reactive investigation.'" (quoting WILLIAM BRATTON, TURNAROUND: HOW AMERICA'S TOP COP REVERSED THE CRIME EPIDEMIC 81 (1998))).

[113] Forman, *supra* note 106, at 6.

[114] *Id.*

[115] *Id.*

[116] *Id.* at 7-8.

perhaps more importantly, it is premised upon a fundamental reconceptualization of the role of citizens in the policing process.[117]

The community policing model has significant advantages over the traditional model of reactive, "warrior-style" policing:

> First, a main drawback of conventional policing, as the individual-self-help proponents have observed, is that it trades off with private methods of controlling and reacting to crime. Community-based solutions sidestep this by incorporating private actors directly into the process of controlling crime. As such, the signal is sent that crime prevention depends not only on the government, but also on the community. Put differently, community strategies emphasize *stewardship*, in that it "calls on citizens to view themselves as responsible for the welfare of the larger community." Second, community-based solutions do a better job of promoting values of order and safety than the public model. When law enforcement is solely responsible for policing, a backlash can develop among residents. Such "top-down" solutions are not particularly effective ways of generating norms. Instead, "when a community responds to a criminal incident, it seeks not merely to restore credibility to the community's conception of the moral order . . . but also to symbolically affirm community norms for others who have not disobeyed them."[118]

The community based policing model not only reduces the antagonism between police officers and citizens, but involves citizens directly in crafting solutions to prevent crimes in their communities and affirming community norms against crime.[119]

The need for community policing against cybercrime arises not because of the antagonistic relationship between law enforcement and computer users, but rather from an understanding that the model can be applied to take advantage of the strengths of third-party actors to prevent cybercrime. Given the fundamental differences between cybercrime and crimes in realspace and the shortcomings of the reactive model of law enforcement, prevention is a crucial element in reducing cybercrime.[120] The emphasis on preventing cybercrime is borne out of the recognition that the traditional reactive model of law enforcement is simply ill-equipped, both normatively and practically, to combat cybercrime.

This is not to say that we would rather prevent cybercrimes, while allowing crimes in realspace to happen and focusing on arresting perpetrators, ex post. In an ideal world, we would prevent all crimes before

---

[117] *Id.* at 8-9.

[118] Neal K. Katyal, *Community Self Help*, 1 J.L. ECON. & POL'Y 33, 46 (2005) (quoting David R. Karp & Todd R. Clear, *Community Justice: A Conceptual Framework*, *in* 2 CRIMINAL JUSTICE 2000: BOUNDARY CHANGES IN CRIMINAL JUSTICE ORGANIZATIONS 323, 331, 337 (Charles M. Friel ed., 2000)) [hereinafter Katyal, *Community Self Help*].

[119] *Id.*

[120] *See, e.g.*, Brenner, *Law Enforcement*, *supra* note 8; Brenner, *Product Liability*, *supra* note 8; Katyal, *Criminal Law in Cyberspace*, *supra* note 5.

they occurred; the question of punishment, ex post, would be moot. Such a goal is obviously unattainable. However, the preventative model is particularly applicable to the problem of crime for two reasons. First, there is a fundamental difference between cybercrime and traditional realspace crime that frustrates the application of traditional models of policing.[121] Second, there is the realization that deterrent strategies may be particularly effective in preventing cybercrimes, vis-à-vis traditional crimes. Increasing the "cost" of committing cybercrime—including measures such as improving software so that it is less vulnerable to attack—has a powerful effect on preventing potential cybercriminals from attempting crimes in the first place.[122]

At first blush, the lack of a tangible, physical location in cyberspace seems to suggest the absence of communities to engage in such self-help remedies.[123] In fact, the opposite may be true:

> [T]he fact that "place" is unfettered online cuts both ways, since it means that opportunities for self-help expand, too. The community in cyberspace may revolve around a number of things, such as a virtual place (eBay); a place in realspace (Georgetown); a concept (Maoism); or even a sport (windsurfing). The proliferation of such communities, and the ease of transacting in each one, suggest a robust potential for community solutions.[124]

Indeed, there is a host of community policing methods already in place in the realm of cyberspace, such as the user rating systems on e-commerce websites like eBay and Craigslist.[125] There is, nonetheless, much work to be done, particularly in the prevention of cybercrimes.

V. OPEN SOURCE SOFTWARE AS A TOOL FOR COMMUNITY POLICING

One important tool that will allow computer users to "patrol" the virtual neighborhoods of the digital world in the attempt to prevent cybercrime is the increased use of open source software. Open source—in the broadest sense—refers to software whose underlying source code[126] is

---

[121] *See supra* Section III.

[122] Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1011.

[123] Katyal, *Community Self Help*, *supra* note 118, at 49.

[124] *Id.*

[125] *See, e.g.*, Craigslist, http://www.craigslist.org (last visited Apr. 21, 2007); eBay, http://www.ebay.com (last visited Apr. 21, 2007).

[126] The term source code refers to the code for the software written in a programming language such as Java, C, or C++, which is easily read by an experienced computer programmer. Before that source code can be used by a computer it must be compiled—translated into machine code, which is simply a string of binary ones and zeroes. Therefore, open source requires the free distribution of not just the source code, but also the machine code. Klaus M. Schmidt & Monika Schnitzer, *Public Subsidies for Open Source? Some*

made available to the public, so, in turn, users are able to alter that code and re-publish it.[127] This stands in contrast to closed or proprietary software, in which, generally, the source code is not available to the user.

A. THE DEVELOPMENT AND USE OF OPEN SOURCE SOFTWARE

Perhaps the best known example of open source software is the Linux operating system developed by Finnish computer science student Linus Torvalds in 1991.[128] The Linux operating system is currently used by over seven million users and is available either as free, open source software or as a commercial software package that includes support and other features.[129] Among its many users are the popular websites Amazon.com and Google, which rely exclusively on Linux.[130] The software is also used to power TiVo digital video recorders, cellphones, and some of the world's most powerful supercomputers.[131] The open source version of Linux is distributed using the Free Software Foundation's GNU General Public License (GPL).[132] A program distributed under the GPL must contain all of its source code.[133] Any user can modify and re-distribute the program; however, any redistribution must also be done according to the terms of the GPL.[134] The GPL license is unique among software licensing schemes—"[w]hile most licenses serve to limit the copies that a licensee may make, the GPL serves to limit the *restrictions* on copying that a licensee can make."[135] Anyone is free to use and modify software distributed under the license, "as long as, in the words of the license preamble, 'you . . . give the

Economic Policy Issues of the Software Market, 16 HARV. J.L. & TECH. 473, 475 (2003).

[127] *See, e.g.*, Yochai Benkler, *Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production*, 114 YALE L.J. 273, 334-45 (2004); Kenneth J. Rodriguez, *Closing the Door on Open Source: Can the General Public License Save Linux and Other Open Source Software?*, 5 J. HIGH TECH. L. 403 (2005); Schmidt & Schnitzer, *supra* note 126, at 475.

[128] Rodriguez, *supra* note 127, at 408. Torvalds set out to create an operating system that would run on the Intel 386 chip architecture. *Id.* He combined the Linux kernel, which he wrote, with other open source code to create a functioning operating system. *Id.* In the ensuing years, as more individuals used and added to the operating system, the culture of Linux—complete with its penguin logo—gained popularity. *See id.*

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *See* Linux Online, http://www.linux.org/info (last visited Apr. 21, 2007).

[133] David S. Evans & Anne Layne-Farrar, *Software Patents and Open Source: The Battle Over Intellectual Property Rights*, 9 VA. J.L. & TECH. 10, ¶ 41 (2004); GNU General Public License, http://www.gnu.org/licenses/gpl.html (last visited Apr. 21, 2007).

[134] GNU General Public License, *supra* note 133.

[135] LESSIG, *supra* note 1, at 59.

recipients all the rights that you have. You must make sure that they, too, receive or can get the source code.'"[136] The effect is a viral propagation of open software—if a user is to take advantage of the openness of the code, he must send along any improvements he makes with the same openness, giving other users the ability to access and modify the source code. A licensee under the GPL cannot simply free-ride on the backs of the previous developers and "close" the code by making the software proprietary. Other prominent examples of open source software include Apache, the most widely used Web server, and Sendmail, which is used to route most e-mail.[137]

The success of open source as a means of community policing against cybercrime lies in the way in which the software distributes the power to identify and correct potential security flaws to the entire community of software users. A key element to developing effective preventative measures against cybercrime is to eliminate the software security flaws that allow criminals to gain access to computer systems and to propagate destructive programs such as viruses, worms, and Trojan horses.[138] To remedy such problems in proprietary closed-source software, the security flaws must be found—by the company that develops the software, by users who discover these flaws and report them to the company, or by cybercriminals who exploit the security flaws to launch an attack.[139] The company must then develop a patch to remedy that problem and release that patch to all users of the software.[140] By contrast, when open source software is released, and again upon the release of each subsequent user-modified version, users are continually scouring the source code for ways to make the software safe from attack.[141]

This continuous search for security flaws and almost-instantaneous release of patches to remedy those flaws means that "[c]omputer platforms such as Linux . . . will have major security advantages . . . [over] closed platforms, such as Windows . . . . Because more people can see the code, the likelihood that security vulnerabilities will be quickly discovered and

---

[136] *Id.*

[137] Evans & Layne-Farrar, *supra* note 133, at 16.

[138] Katyal, *Community Self Help*, *supra* note 118, at 54-55.

[139] *Id.*

[140] *Id.*

[141] The aim of this Comment is not to undertake an empirical comparison of the security features of open source and proprietary software, but rather to draw upon evidence of the success of open source software in preventing unauthorized access and disruption of computer systems and to advocate expanding the use of open-source software, particularly in the operating system and Internet browser markets.

patched rises."[142] Particularly, "if a program is ubiquitous, like a computer operating system, the open source proponents are right that the multitude of users will examine the code[,] reveal its flaws" and help to craft ways to fix those flaws.[143] As President Clinton's Technical Advisory Panel pointed out, "[A]ccess by developers to source code allows for a thorough examination that decreases the potential for embedded trap doors and/or Trojan horses."[144] Tellingly, in 2001, Microsoft's closed source web server—IIS—was the most frequently targeted server by hackers, despite the fact that there were a far larger number of Apache web servers in use.[145]

The use of open source software to combat cybercrime also brings with it the same normative values as community policing, namely the erosion of the traditional barrier between law enforcement and citizens:

> Open-source programs involve the user in the process of security, instead of relegating it to someone else. Closed-source software creates the same type of "we/they syndrome" as conventional policing does. There is just not much impetus to try to come up with solutions to Windows XP's security flaws when one cannot even access the code. The closure of code sends a signal, and that signal is that Microsoft will take care of your security problems. Such centralized solutions are no doubt successful under certain conditions, but, as the self-help proponents rightly point out, they can also be efficient. In this way, the Linux community, often viewed as a bunch of anti-market sympathizers, have much in common with the market-based economists who emphasize self-help on efficiency grounds.[146]

Just as community policing initiatives empower residents to take responsibility for the security of their communities, open source software empowers computer users to proactively take charge of identifying and

---

[142] Neal K. Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261, 2265 (2003). For example, when users discovered a security vulnerability in the Linux operating system known as the "Ping of Death" that allowed a remote user to flood the computer and cause it to crash, a patch fixing the problem was posted within hours of the problem's discovery, far more quickly than Microsoft was able to identify and patch the same problem in Windows. *Id.* at 2265 n.14; *see also* TRUSECURE, OPEN SOURCE SECURITY: A LOOK AT THE SECURITY BENEFITS OF SOURCE CODE ACCESS (2001), *available at* https://www.redhat.com/whitepapers/services/Open_Source_Security5.pdf.

[143] Katyal, *Community Self Help*, *supra* note 118, at 54.

[144] PRESIDENT'S INFO. TECH. ADVISORY COMM., DEVELOPING OPEN SOURCE SOFTWARE TO ADVANCE HIGH END COMPUTING (2000), *available at* http://www.egovos.org/rawmedia_repository/abfd4d56_7673_499a_b4aa_6cafe77dcaff?/document.pdf.

[145] David A. Wheeler, Why Open Source Software/Free Software (OSS/FS, FLOSS, or FOSS)? Look at the Numbers!, Nov. 14, 2005, http://www.dwheeler.com/oss_fs_why.html (last visited Apr. 21, 2007). Many firms are switching from Microsoft to Apache web servers because of the large number of viruses written specifically for the Microsoft software. *Id.*

[146] Katyal, *Community Self Help*, *supra* note 118, at 54-55.

correcting security breaches, rather than relying on the distributors of proprietary software.

B. GOING FORWARD

Open source software is not, however, a panacea that can be easily and seamlessly deployed to stem the tide of cybercrime. Important questions must be answered about the organizational structure of a potential open source community policing effort. First, will individuals be motivated to contribute to open source projects? Second, will software corporations be willing to abandon the proprietary software model in order to devote more resources to open source software? And finally, what is the proper role of government, if any, in promoting the increased use of open source software? The answers to each of these questions reveal not only a promising future for effective preventative measures against cybercrime, but also an alternative to firm and market driven economies that dominate the landscape of modern industry.

1. Individual Users

Looking first to individuals, there is persuasive evidence that individual users can and will invest their time and resources in creating and updating open source software programs to protect against cybercrime.[147] First, the emergence of the model of peer production (of which open source software is one example) is tied to the emergence of the networked, information age.[148] In essence, the interconnectivity of millions of computer users, which contributes to the scope and power of cybercrime, is a powerful tool for allowing individuals to collaboratively work on open source software projects.[149] As one scholar points out, "[U]biquitous computer communications networks are bringing about a dramatic change

[147] In the context of open source software, the term "user" can refer to two different groups of people—those who use the software merely for its primary function and those who may use the software, but also work with the source code to improve and change the software itself. In discussing the role of users in shaping and improving open source software, this Comment focuses on the latter group. However, that does not mean that the benefits of open source programs accrue only to such advanced users. For example, the Firefox Internet browser, discussed *infra*, notifies all users (including those who merely use it to surf the Internet) of updates to the software—which are the product of the collaborative efforts among those who choose to tinker with the source code. In a very simple process, all users can download those updates (including important security patches) and improve the functionality of their software.

[148] *See* Yochai Benkler, *Coase's Penguin, or, Linux and The Nature of the Firm*, 112 YALE L.J. 369, 404 (2002).

[149] *Id.* at 383.

in the scope, scale, and efficacy of peer production."[150] In short, programmers, connected via the Internet, are able to freely and cheaply exchange information.[151] This exchange of information allows users to quickly and easily identify areas of production (including security flaws in software that create avenues for cybercrime) and contribute their productive efforts to the overall open source project.[152]

The second important characteristic is the size, or granularity, of the tasks performed by each user in an open source community. Given the number of users collaborating on an open source project, the size of the individual tasks that each user must perform is quite small. Thus the motivation necessary to compel each user to complete that task is correspondingly small.[153] When a project "is broken into little pieces, each of which can be performed by an individual in a short amount of time, the motivation to get any given individual to contribute need only be very small."[154] If the creation of an operating system requires fifty thousand man hours of production, and the community of users numbers ten thousand, it is far easier to motivate each one to contribute five hours of her time than it would be—absent a firm-based command notion or a market-based structure—to motivate fifty individuals to perform one thousand hours of work each. This is particularly true of users in the open source community

---

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.* at 378.

[154] *Id.*

> This suggests that peer production will thrive where projects have three characteristics. First, they must be modular. That is, they must be divisible into components or modules, each of which can be produced independently of the production of the others. This enables production to be incremental and asynchronous, pooling the efforts of different people, with different capabilities, who are available at different times. Second, the granularity of the modules is important and refers to the sizes of the project's modules. For a peer production process to pool successfully a relatively large number of contributors, the modules should be predominantly fine-grained, or small in size. This allows the project to capture contributions from large numbers of contributors whose motivation levels will not sustain anything more than small efforts toward the project. . . . In addition, a project will likely be more efficient if it can accommodate variously sized contributions. Heterogeneous granularity will allow people with different levels of motivation to collaborate by making smaller- or larger-grained contributions, consistent with their levels of motivation. Third, and finally, a successful peer production enterprise must have low-cost integration, which includes both quality control over the modules and a mechanism for integrating the contributions into the finished product. If a project cannot defend itself from incompetent or malicious contributions and integrate the competent modules into a finished product at sufficiently low cost, integration will either fail or the integrator will be forced to appropriate the residual value of the common project—usually leading to a dissipation of the motivations to contribute, ex ante.
>
> *Id.* at 378-79.

who are often motivated to improve and distribute software for non-pecuniary interests such as increased reputation in the programming community.[155]

At this point, it is important to understand the nature of open source software itself. A common misconception regarding open source is that the software is only designed for savvy computer users or those who are "in the know" about a range of products beyond those in common use (particularly those offered by the dominant players in the software market such as Microsoft). At its simplest, this assumption is false. Open source programs, including the Linux operating system and functionality software such as the Firefox browser and the OpenOffice suite, are no more difficult to use for even the novice computer user and—importantly—are often available for free.[156] Yet, it reveals an important challenge for a model of community policing built upon increasing the use of open source: not only making that software more accessible to the public, but increasing the public use of that software.

However, in recent years, open source software such as Linux and Firefox have gained increasing use among both savvy and novice computer users. These developments provide an important glimpse into the efficiency and "user-friendliness" of open source projects and illustrate the power of large numbers of individuals, each completing small scale tasks, to produce powerful results, despite the absence of command behavior from a firm or state organization. It is helpful to look at a few of the most prominent examples of peer-produced projects to see not only the capacity for organization and collaboration among a large group of individuals, but also the accessibility of these programs to even the most novice computer user.

a. Wikipedia—The Collaborative Encyclopedia

The first example is the Wikipedia project, an ambitious attempt to create an Internet-based encyclopedia whose content is continually written and edited by its users.[157] The project uses a collaborative software, Wiki, that is a markup language similar to HTML and allows multiple people to

---

[155] David McGowan, *Legal Implications of Open-Source Software*, 2001 U. ILL. L. REV. 241, 276 (2001).

[156] This again ties into the dual conception of open source "users" discussed *supra* in note 147. It is true, however, that only those users who are able to modify the source code of the software can actually remedy potential security breaches. Nonetheless, even the most unskilled computer user can make use of open source software, even if they do not actively engage in retooling the software and posting those revisions for future downloading.

[157] *See* Wikipedia, http://www.wikipedia.org (last visited Apr. 21, 2007).

edit a single document and to link it to other, related documents.[158] Begun in 2000 with a small number of volunteers, the site now features over a million entries in languages ranging from English to Luxembourgish to Tagalog.[159] All users of the site are free to add articles and to update or edit existing articles.[160] If a user feels that there should be an entry on the pygmy hippopotamus, she is free to add that content to the site. The unique feature of Wikipedia, vis-à-vis traditional encyclopedias, is that there is no central editor who reads the content added by users checking for misinformation.[161] Instead, users themselves must be alert for mistakes in articles and are encouraged to correct those mistakes as they encounter them.[162] Just as the power to correct bugs in open source software is spread among all of the users who access the source code, the editing power of the encyclopedia is distributed over the entire base of users of the site.

b. Firefox—A Better Browser?

The second example of the power of open source collaboration is the development of the Mozilla Firefox web browser, which stands as a shining example of the potential to create open source software solutions to the problem of cybercrime. The Firefox browser is the product of the Mozilla Foundation, spun off from America Online in 2003 as one of the last vestiges of Netscape, the Internet browser that dominated the competitive landscape before the introduction of Microsoft's Internet Explorer.[163] The browser is built upon an open source architecture where programmers and developers are given access to the source code, not only to search for security flaws, but also so that they may write additional plug-ins and extensions that increase the browser's functionality.[164] While its market share still pales in comparison to the near-ubiquitous Internet Explorer, Firefox has captured an increasingly large segment of the market, driving Microsoft's share below 90%.[165] The software is touted for its security

---

[158] *Id.*

[159] *Id.*

[160] *Id.*

[161] *See id.*

[162] *Id.*

[163] Walter Mossberg, *Security, Cool Features of Firefox Web Browser Beat Microsoft's IE*, WALL ST. J., Dec. 30, 2004, at B1.

[164] *Id.*

[165] Thomas Claburn, *Firefox Eats More Microsoft Market Share*, INFORMATIONWEEK, Mar. 18, 2005, http://www.informationweek.com/story/showArticle.jhtml?articleID=159902316.

features and its resistance to viruses and other forms of unauthorized disruption.[166]

Given the nature of the software market and the enabling characteristics of the Internet, peer-produced projects such as open source software systems may emerge as a viable alternative to the traditional firm-based theory of economic behavior.[167] The emergence of open source software projects, shaped not by the top-down leadership of a dominant firm, but by the collaboration of many peer contributors has forced a re-thinking of Coase's firm-based theory of production, one of the bedrock principles of modern business operation.[168] Open source programmers do not choose to participate in a project because their boss instructed them to do so, nor do they rely on the presence of a market price for their work which provides the prospect of either present or future monetary returns.[169] As Benkler suggests, the peer production of open source software projects may in fact have a unique advantage over traditional, firm-based theories of production, allowing programmers to "scour larger groups of resources in search of materials, projects, collaborations, and combinations than is possible for firms or individuals who function in markets."[170]

There is also a responsibility incumbent upon the developers and users of open source software to create programs that can be used by a greater number of computer users (users, here, in the traditional sense of the term, including those who only make use of the software for its intended purpose). For many, open source programs such as Linux are seen as more complicated and risky than traditional proprietary programs, such as the Microsoft Windows operating system. This perception is part myth and part truth. In the future, this perception may even cease to be true: if open source developers work to create more programs—like Firefox—that are accessible to even the most unsophisticated computer users, the demand for such products and the use of products better equipped to prevent cybercrime will only increase.

---

[166] Mossberg, *supra* note 163.

[167] Benkler, *supra* note 148, at 372. In the late 1930s, Ronald Coase wrote *The Nature of the Firm*, describing the emergence of firms as a dominant market force. Ronald Coase, *The Nature of the Firm*, 4 ECONOMICA 386 (1937). In general terms, Coase introduced the concept of transaction costs—costs associated with defining and enforcing property rights—and argued that firms emerge where the transaction costs of operating as an aggregate, command-driven unit are less than when individuals could operate autonomously in the market. *See id.* Conversely, a firm will stop growing when the transaction costs incurred by such growth outweigh the gains received from growing. *See id.*

[168] Benkler, *supra* note 148, at 372.

[169] *Id.*

[170] *Id.* at 376-77.

2. Corporations

The question of how to motivate users to participate in the improvement and expand the use of open source software is not the only dilemma. The next step is how to encourage corporations—still the producers of most software programs—to embrace open source. For software companies, proprietary software is an extremely profitable enterprise.[171] It would be folly to suggest that distributors of proprietary software abandon their business model to embrace open source. By "giving away" the source code to software, companies lose the very profit-generating benefits that flow from closed-code, proprietary software. However, there may be feasible solutions that allow for the greater introduction of open source software. One such solution could be for Microsoft—the dominant producer of operating system and productivity software for end users—to give programmers and developers greater access to the source code for Internet Explorer, which is currently bundled with its Windows operating system.[172] Without revealing the source code for Windows—the lifeblood of Microsoft's revenue stream—the company could give greater transparency to its Internet browser, allowing developers to scour the source code for security flaws before they were exploited by potential criminals. This raises the question of whether making the source code for Internet Explorer open to all would not only benefit those who seek to prevent cybercrime, but also those who perpetrate cybercrime. Would we, in effect, be letting the fox into the henhouse? Of course, making the source code available to all could increase the ability of cybercriminals to exploit potential weaknesses, but it would also vastly increase the ability and the motivation of users to test and update the source code in order to fix security flaws.

Indeed, drawing on the success of companies such as RedHat (a for-profit distributor of Linux software and technical support) and IBM (which has also become involved in the distribution of Linux platform), an increasing number of firms are realizing the potential of the open source

---

[171] For example, Microsoft, the distributor of the dominant Windows operating system and Internet Explorer, earned $39.79 billion in revenue for the fiscal year ending June 30, 2005. Fast Facts About Microsoft, http://www.microsoft.com/presspass/inside_ms.mspx #EEMAC (last visited Apr. 21, 2007). This revenue stream generated $12.25 billion in profits for the company. *Id.*

[172] Interestingly, in January 2006, Microsoft offered to reveal some of the source code for its Windows Server software in response to threatened sanctions by European Union antitrust regulators. *See* Dawn Kawamoto, *Microsoft Offers Up Source Code in EC Dispute,* CNET NEWS.COM, Jan. 31, 2006, http://news.com.com/Microsoft+offers+up+source+code +in+EC+dispute/2100-1014_3-6030879.html.

market.[173] Venture capital firms invested over $400 million into open source companies over an eighteen month period dating from 2004 to 2005, a sum that seems even larger given the capital-efficient nature of open source firms, which do not require massive armies of salespeople or developers.[174] The key is to further develop this notion that the open source model is not an anathema to traditional notions of sales and profit. Instead, drawing on the experience of Linux distribution, software companies can and should move toward the open source model.

3. Government

A final question concerns the role of government in promoting community policing through the use of open source. Unlike most policy choices, the increased use of open source software is one that must begin in the private sphere—among software distributors and, more importantly, those who write and use open source software. However, the government can and should take a role in furthering this end.[175]

A potential first step is the subsidy of open source software developers. Given the obvious deleterious effects of cybercrime—both in terms of monetary losses and the diversion of law enforcement resources away from other forms of crime—government agencies (both federal and state) have a vested interest in promoting the spread of open source software as a defense against cybercrime. Government subsidies would give open source developers additional capital to expand the range and capabilities of platforms such as Linux and Firefox. Further, by encouraging the adoption of open source software, perhaps through tax breaks or some other indirect subsidy, governments can motivate the increased use of these products, thus decreasing the number of targets of cybercrime.[176]

---

[173] Sarah Lacy, *Open Source: Now It's an Ecosystem*, BUSINESSWEEK, Oct. 3, 2005, http://www.businessweek.com/technology/content/oct2005/tc2005103_0519_tc_218.htm.

[174] *Id.*

[175] For example, China—one of the largest and fastest growing information technology markets—announced plans to create a domestic software industry modeled on Linux, which would become the national standard. *China to Invest in Linux-based Software*, CNN.COM, Nov. 5, 2003, http://www.cnn.com/2003/TECH/biztech/11/05/china.linux.reut/index.html.

[176] *See* Dan M. Kahan, *The Logic of Reciprocity: Trust, Collective Action, and Law*, 102 MICH. L. REV. 71, 98 (2003) ("[T]he government will likely need to take a more active stance in promoting reciprocity. As the examples of the university, the industrial campus, and open-source programming all illustrate, collaborative intellectual production depends on ancillary systems of material compensation for reciprocal producers. Private actors—including philanthropists in the case of universities, and commercially motivated firms in the case of industrial campuses—will be motivated to contribute part of what it costs to operate such systems, but they are unlikely to contribute the optimal amount. Indeed, government

Open source software platforms represent a viable tool to implement effective community policing solutions against cybercrimes. Just as community policing in realspace increased the accountability of citizens and diffused the responsibility for preventing crime among the population, so too will the use of open source software in the virtual realm.

VI. CONCLUSION

The Linux penguin doesn't look like much of a crime-fighter. He's a little portly and looks as if he would be much happier sliding around the ice than chasing down criminals. Yet this logo, and the open source operating system which it represents, offer a glimpse into a powerful force for preventing crime in cyberspace. The current strategies designed to fight cybercrime are failing. The reactive, investigative model—developed over the millennia as a response to localized crimes committed by a single perpetrator against a single victim—is ill-equipped to respond to criminal acts that can span the globe in a matter of seconds and affect thousands, if not millions of victims.

Just as law enforcement officials were able to tap into urban communities as a powerful resource for developing crime-prevention strategies, the time has come to look to virtual communities as a way to stem the tide of cybercrime. Although these virtual communities exist only as a seemingly-random string of ones and zeroes beamed around the globe and reconstituted into images, pictures, and sounds on computer screens, they retain many of the same features as their tangible, realspace counterparts—most notably, a sense of common interest among their members.

The use of open source software is a unique way to apply the community policing model to cybercrime. Just as neighborhood watch programs put "eyes on the street" to deter crimes like mugging, rape, and murder, open source software allows programmers and developers to monitor the code which shapes cyberspace and deters cybercrimes.

---

subsidization has traditionally played a vital role in securing the societal benefits of reciprocal production in the university. Similar efforts of public support—perhaps in the form of tax benefits for firms that invest in open-source technologies—are likely to be necessary to realize the full potential of the internet as a catalyst of reciprocal production."); *see also* LESSIG, *supra* note 1, at 247 ("What reason does the government have for supporting closed code, when open code is as powerful and the externalities from using open code would benefit others? If the PCs that the government owned ran something other than Windows, then the market for these alternative platforms would be wildly expanded. And if the market for alternatives were strong, then the benefits from building for these alternatives would be strong as well.").