Volume V - Article 1

TOWARD A CRIMINAL LAW FOR CYBERSPACE: PRODUCT LIABILITY AND OTHER ISSUES

Susan W. Brenner[1]

Fall 2004

TABLE OF CONTENTS

I. INTRODUCTION 1

II. CYBERCRIME, CYBERRULES 8

A. CYBERCRIME 9
1. Real-world Crime 9
2. Real-World Model 11
3. Cybercrime 14
4. Cybercrime Model 18
(a) Why 26
(b) How 29

B. CYBERRULES 35

C. "USERS" AND "ARCHITECTS" 50
1. "Users" 51
(a) Assumption of Risk 51
(b) Complicity 55
2. "Architects" 63
(a) Civil Products 68
(b) Civil Liability 78

III. TOKUGAWA CYBERSPACE 89

IV. CONCLUSION 108

---

[1] NCR Distinguished Professor of Law & Technology, University of Dayton School of Law, Dayton, OH. Email: Susan.Brenner@notes.udayton.edu. Website: http://www.cybercrimes.net.

I. Introduction

Hidden in the Net is the mystery of the Invisible Hand—control without authority.[2]

This article is a speculation – an exploration of the advisability of incorporating certain principles into the criminal law governing cyberspace.[3] Why is such an exploration necessary? Why, in other words, is it necessary to consider "a criminal law for cyberspace"?

The migration of a substantial portion of human activities into cyberspace erodes the efficacy of the traditional model of law enforcement – the constellation of rules, procedures and personnel we use to maintain "order" in discrete societies.[4] Societies are but one type of system composed of autonomous entities; all such systems must maintain a baseline of internal order if they are to carry out the processes that are necessary for the system to survive.[5]

---

[2]Kevin Kelly, Out of Control: The New Biology of Machines, Social Systems, and the Economic World 26 (1994).

[3]For the proposition that distinct principles of criminal law should govern cyberspace, *see* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 10 B.U.J. SCI. & TECH. L. 1 (2004) [hereinafter Brenner, *Distributed Security*]; Susan W. Brenner, *Toward A Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 RUTGERS COMPUTER TECH. L.J. 1 (2003) [hereinafter Brenner, *A New Model of Law Enforcement?*].

[4]*See* Brenner, *Distributed Security*, *supra* note 3; Brenner, *A New Model of Law Enforcement?*, *supra* note 3. *See also* World Federation of Scientists, Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar 9 (August 2003), *at* http://www.unicttaskforce.org/community/documents/257947542_wfs_cybersecurity.pdf (proposing a criminal law for cyberspace).

[5]*See* Brenner, *Distributed Security*, *supra* note 3:

> Order . . . means that a sufficient measure of control has been established over the environment within which a system operates and the . . . entities who comprise it so that the latter can successfully discharge the tasks necessary for the perpetuation of the system. If a . . . system is to survive, it must . . . ensure the continuity of a populace of the entities of which it is comprised. For biological systems, this means ensuring (a) that its constituent entities have the necessities . . . they need to survive and to reproduce themselves; (b) that their offspring achieve adulthood and

Like all systems composed of autonomous entities, human societies are self-organizing: They use rules to create and sustain internal order.[6] Like all self-organizing systems, human societies employ constitutive rules for this purpose. [7] Constitutive rules – much like the rules of a board game – set the parameters of acceptable behavior on the part of the entities populating the system.[8]

Human societies have also heretofore operated as bounded systems; that is, they have been situated in a delimited spatial area and have been composed of a defined populace (e.g., "the people of Rome," "the citizens of Athens," "the American public," and so on).[9] These spatial and population constraints facilitate the operation of the constitutive rules that maintain internal order. Spatial and demographic isolation make it easier to socialize the individuals populating a specific system so that most of them accept and abide by its constitutive rules; on the other hand, spatial isolation also makes it easier to identify, and to suppress, those who violate these rules.[10] The inevitability of such violations differentiates human societies from other self-organizing systems. Unlike the entities that populate most biological systems and every artificial system heretofore created, humans are highly intelligent and, as a result, inhabit systems constituted by rules of their own design.[11] While the need to sustain internal order necessitates that there be functional continuities in the rules that comprise all human systems, the

---

are successfully incorporated into the system; and (c) that these discrete entities and the system itself are protected from the depredations of competitors and predators.

[6] *See id.*

[7] *See id.*

[8] *See id.*

[9] *See id.*

[10] *See id.*

[11] *See id. See also* Peter Berger & Thomas Luckmann, *Society as a Human Product* in Social Theory: Multicultural and Classic Readings 384, 384 (Charles L. Lemert ed., 1999) ("Social order exists *only* as a product of human activity").

forms these rules take can vary from system to system and can be mutable within a system.[12] Thus, the variability and mutability of the constitutive rules employed by human systems can result in their being perceived as nonbinding by certain individuals who populate a system; this option is not available to entities, such as social insects, which are driven by biological imperatives.[13] Ant societies, for example, employ a repertoire of constitutive rules for creating intricate social structures and for carrying out highly complex activities; yet, no ant is capable of deviance from the constitutive rules. Ants have war, but not crime.[14] Humans have both.

Along with maintaining internal order, systems must also maintain an acceptable level of external order.[15] External order governs a system's relationship with its environment; "environment" encompasses both the physical context within which a system functions and the "alien" entities that can threaten a system's survival by attacking or competing with its populace for essential resources.[16] Every system will therefore also have rules that structure its interactions with its environment; for example, ant colonies have rules governing war with other colonies and the process of relocating and founding colonies.[17] The rules governing internal and external order do not operate independently; instead, they interact and evolve, allowing the system to adapt to changes in its environment.[18]

The focus of this discussion, however, is on internal order. Due to humans' unique capacity to deviate, i.e., to contumaciously disregard the constitutive rules that maintain order in

[12]*See* Brenner, *Distributed Security*, *supra* note 3.

[13]*See id.*

[14]*See id.*

[15]*See id.*

[16]*See id.*

[17]*See id. See also* George C. Homans, The Human Group 88-91 (1950).

[18]*See* Brenner, *Distributed Security*, *supra* note 3.

a human social system, human systems, unlike other self-organizing collective systems, cannot rely solely on constitutive rules to maintain internal order.[19] Human systems add another set of rules: proscriptive rules that impose consequences upon those who violate constitutive rules.[20] Proscriptive rules dictate that violating constitutive rules will result in the imposition of sanctions such as death, corporal punishment, banishment, incarceration, or the like.[21] They are founded on the assumption that sanctioning those who violate constitutive rules maintains internal order by preventing such violations in the future.[22] This assumption is based on two propositions: (i) sanctions prevent violations by presenting the populace with the simple choice of obeying the rules or suffering unpleasant consequences;[23] and (ii) those who violate constitutive rules will be identified, apprehended and sanctioned.[24]

Since the efficacy of proscriptive rules depends upon apprehending and sanctioning violators, proscriptive rules must be accompanied by an enforcement mechanism.[25] In the several millennia since human social systems emerged, societies have accomplished this in

---

[19]*See id.*

[20]*See id.*

[21]*See id. See also infra* Part II(B).

[22]*See* Brenner, *Distributed Security*, *supra* note 3, at 55-60. *See also infra* Part II(B).

[23]*See* Brenner, *Distributed Security*, *supra* note 3, at 55-60. This proposition incorporates the concept of deterrence, which has two aspects: specific deterrence and general deterrence. *See, e.g.*, WAYNE R. LAFAVE, 2 SUBSTANTIVE CRIMINAL LAW § 1.5 (2d ed. 2003). Specific deterrence refers to the effect on the individual offender; "criminal punishment aims to deter the criminal himself . . . from committing further crimes, by giving him an unpleasant experience he will not want to endure again." *Id.* § 1.5(a)(1). General deterrence refers to the effect on others; "the sufferings of the criminal for the crime he has committed are supposed to deter others from committing future crimes, lest they suffer the same unfortunate fate." *Id*. § 1.5(a)(4).

[24]*See* Brenner, *Distributed Security*, *supra* note 3, at 55-60; Brenner, *A New Model of Law Enforcement?*, *supra* note 3, at 14-25.

[25]*See* Brenner, *Distributed Security*, *supra* note 3, at 55-60.

different ways with varying degrees of effectiveness. For centuries, Anglo-American societies relied upon citizen enforcement. In Britain at the time of Alfred the Great, every male was

> required to participate in . . . the tything system. A tything was a group of ten families, headed by a `tythingman.'. . . It was each tythingman's duty to raise the `hue and cry' when a crime was committed, to collect his neighbors and to pursue a criminal. . . . If such a group failed to apprehend a lawbreaker, the tything could be required to pay a fine. . . . [26]

The Normans essentially kept this system in place.[27]

In 1285, the Statute of Winchester introduced a modified approach by establishing citizen patrols in the large towns of England. Men between ages fifteen and sixty were "required to perform watch service . . . [and were made] responsible for . . . apprehending anyone who committed a crime. . . . [T]he entire community of able-bodied males was required to join in the pursuit of any wrongdoer. A failure to participate . . . would result in punishment."[28] For the next five centuries, policing in England and in the American colonies consisted of this "watch and ward" system.[29] Nevertheless, citizen commitment slowly weakened and it became common

[26]CYRIL D. ROBINSON ET AL., POLICE IN CONTRADICTION: THE EVOLUTION OF THE POLICE FUNCTION IN SOCIETY 19 (Contributions in Criminology and Penology, Series No. 44, 1994).

[27]*See id*. at 93.

[28]*Id.* at 20 (notes omitted).

[29]*Id. See also* BRUCE L. BERG, POLICING IN MODERN SOCIETY 29-32 (Butterworth-Heinemann ed., 1999). "Law enforcement in the Founders' time was a duty of every citizen. Citizens were expected to be armed and equipped to chase suspects on foot, on horse, or with wagon whenever summoned." Roger Roots, *Are Cops Constitutional?*, 11 SETON HALL CONST. L.J. 685, 692-93 (2001).

to hire substitutes, who were generally "too old to be of any value."[30] By the end of the eighteenth century crime rates were increasing steadily, exacerbated by the "vast migration to urban areas" resulting from the Industrial Revolution.[31] The British and American publics opposed police forces, fearing they would infringe on individual freedom, but their opposition was to no avail.[32] In 1829, Parliament passed Sir Robert Peel's Metropolitan Police Act and created a tax-supported police force for the London area.[33]

> [T]he Metropolitan Police created by this legislation provided the model for modern policing. . . . First, the officers were independent from the courts. . . . Second, the force was uniformed, and quasi-military in organization. Patrols were assigned to constables, who were supervised by sergeants, who in turn reported to inspectors, who were under the command of superintendents, who reported to the commissioner. Third, policing was a full-time occupation, and officers were not allowed to . . . accept . . . private payments for their work.[34]

Forces modeled after the Metropolitan Police spread through England and America and eventually around the world.[35] For at least the last century, the paradigm has been a hierarchical, quasi-military model in which authority is centralized and orders move down a chain of command.[36] The primary focus of these agencies has been to react to completed crimes; they

---

[30]ROBINSON, *supra* note 26, at 21. *See also* THE ROLE OF POLICE IN AMERICAN SOCIETY: A DOCUMENTARY HISTORY 4 (Bryan Vila & Cynthia Morris eds., 1999).

[31] ROBINSON, *supra* note 26, at 21.

[32]*See, e.g.*, David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1201-07 (1999).

[33]*Id.* at 1202.

[34]*Id.* at 1202-1203 (notes omitted).

[35]*See, e.g.*, BERG, *supra* note 29, at 27-34.

[36]*See* Brenner, *Distributed Security*, *supra* note 3, at 63-64.

apprehend offenders and work with the judicial system to ensure they are appropriately sanctioned.[37]

As a result of shifting the responsibility for enforcing the constitutive rules to specialized law enforcement agencies, civilians, who were not part of these agencies, gradually surrendered responsibility for maintaining internal security.[38] Today, in most if not all countries, citizens see internal security as the exclusive province of law enforcement professionals. Citizens may lock their doors and install burglar alarms because they realize this is necessarily an imperfect system, but they generally feel no personal responsibility for reacting to, or for preventing, crime.[39]

Since this model of law enforcement evolved to deal with crime occurring in the real, physical world, it incorporates certain assumptions about the nature of crime.[40] These assumptions reflect the nature of real-world crime with a fair degree of accuracy, making the model a satisfactory means for dealing with real-world violations of proscriptive rules; it maintains an acceptable, albeit imperfect, level of internal order within contemporary human

---

[37]*See id*. *See also* DAVID GARLAND, THE CULTURE OF CONTROL: CRIME AND SOCIAL ORDER IN CONTEMPORARY SOCIETY 34 (2001): Model assumes "crime control must be a specialist, professional task of 'law enforcement,' oriented to the . . . pursuit and processing of…offenders. No need…to encourage private action. No need to involve the public . . . No need for . . . prevention. All that was required was a framework of legal threats and a reactive response."

[38]*See, e.g.*, GARLAND, *supra* note 37. *See also* Brenner, *Distributed Security*, *supra* note 3, at 64.

[39]*See, e.g.*, GARLAND, *supra* note 37, at 32:

> By the middle . . . of the twentieth century, . . . police . . . had come to occupy a dominant position . . . and the public's standard response to victimization was increasingly to file a report with the police. . . . [T]he crime control activities of citizens . . . tended to atrophy . . . The presence of professionals tended to de-skill the people and to relieve them of the sense that crime control was their responsibility. Crime became something that 'the authorities' should do something about . . . .

[40]*See id.*

societies.[41] However, because it assumes real-world crime, this model is not a satisfactory means of dealing with cybercrime; the assumptions that hold for real-world crime do not hold for crime that occurs in or is mediated through cyberspace.[42] The inapplicability of these assumptions and the consequent inefficacy of our current approach to law enforcement requires us to devise an alternative model for cybercrime, one that supplements the traditional, reactive approach to law enforcement.[43]

Part II of this article outlines the traditional model's assumptions about real-world crime and explains why these assumptions do not hold for cybercrime. It also outlines an alternative model of law enforcement, one that emphasizes preventing crimes instead of reacting to them, and explains why this is a preferable strategy for dealing with cybercrime.[44] Part III explains how several new principles of criminal law can be used to operationalize this model, which represents a non-hierarchical system of distributed security. Finally, Part IV provides a brief conclusion.

II. CYBERCRIME, CYBERRULES

The prevailing model of law enforcement evolved to deal with real-world crime – the only kind of crime societies encountered until recently – and therefore makes certain assumptions about crime.[45] As Part II(A) explains, the model incorporates four assumptions, all

---

[41] *See id.*

[42] *See id.*

[43] *See id.*

[44] It is also a superior strategy for dealing with real-world crime; when Sir Robert Peel founded the Metropolitan Police, one of his goals was to have officers prevent crime. *See id*. at 221 n.9. "But this preventive function came to be interpreted as the deterrent effect of a police presence…and the apprehension of offenders eventually took operational priority." *Id.*

[45] *See, e.g.*, Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J. L. & Tech. 3, 56 http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf.

of which tend to hold for real-world crime but none of which are valid for cybercrime. Since these assumptions structure the model's approach to "crime," the model is ill-equipped to deal with cybercrime. Parts II(B) and II(C) therefore outline an alternative model of law enforcement which can effectively be used in the fight against cybercrime.

A. CYBERCRIME

Unlike a physical frontier, the Net is truly infinite.

The more it is inhabited, the wilder it becomes. . . .[46]

Parts 1 and 2 below outline four characteristics of real-world crime and show how they shaped the traditional model of law enforcement. The following sections explain why cybercrime shares none of these characteristics and why it is therefore necessary to develop a new approach for dealing with online crime.

1. Real-world Crime

Being situated in a physical environment, real-world crime possesses four relevant characteristics: proximity, scale, physical constraints, and patterns.

Perhaps the most fundamental characteristic of real-world crime is that the perpetrator and the victim are necessarily physically proximate to each other when the offense is committed or attempted. It is, for instance, impossible to rape or realistically attempt to rape someone if the rapist and the victim are fifty miles apart. Likewise, in a non-technological world, it is physically impossible to pick someone's pocket, or to rob or defraud someone out of his property, if the thief and victim are in different cities, different states, or different countries.

Further, the scale of real-world crime is limited, as it tends to be one-to-one crime. A one-to-one crime is an event that involves only one perpetrator and one victim. During the event

[46]Chris Hables Gray, Cyborg Citizen 134 (2001).

the perpetrator focuses all of her attention on consummating that crime. When it is complete, the perpetrator can move onto another crime and another victim. Like proximity, the one-to-one character of real-world crime derives from the constraints physical reality imposes upon human activity: A thief cannot pick more than one pocket at a time, a forger cannot forge more than one document at a time, and, prior to the rise of firearms, it was exceedingly difficult for one to cause the simultaneous deaths of more than one person. Real-world crime therefore tends to be serial crime.[47]

Real-world crime is also subject to the physical constraints governing activity in the real world. Every crime, even street-level drug dealing or prostitution, requires a level of preparation, planning, and implementation if it is to succeed. A bank robber must visit the bank to familiarize herself with its layout, security, and routine; this exposes her to public scrutiny, which can lead to her identification and apprehension after she commits the crime. The same is true of the robbery itself; while in the bank, the robber leaves trace evidence and subjects herself to observation. As she flees the scene of the crime, she is again exposed to public view and risks being identified. In addition to these obvious risks, the robber probably needed to secure a weapon and some type of disguise before the robbery and would require help disposing of the cash afterward. Each step takes time and effort, thereby incrementally augmenting the exertion required to commit the crime and increasing the risk involved in its commission.

Finally, over time it becomes possible to identify the general contours and incidence of the real-world crimes committed in a society. Victimization tends to fall into demographic and

[47]The one-to-one nature of real-world crime is more a default than an absolute; exceptions occur, especially as to the number of perpetrators. Many crimes can involve multiple perpetrators. While many-to-one deviations from the one-to-one model have occurred for centuries, one-to-many deviations were rare prior to the use of technology. *See* Brenner, *Distributed Security*, *supra* note 3.

geographic patterns for two reasons. First, only a small segment of a functioning society's populace will persistently engage in criminal activity. Those who fall into this category are apt to be from economically-deprived backgrounds and reside in areas that share geographic and demographic characteristics. They will be inclined to focus their efforts on those with whom they share a level of physical proximity because they are convenient victims; consequently, much of a society's routine crime will be concentrated in identifiable areas. The second reason crime falls into patterns is that each society has a repertoire of crimes – rules which proscribe behaviors ranging from more to less serious in terms of the harm each inflicts. Theft yields a loss of property, rape yields nonconsensual sexual intercourse, murder yields a loss of life, and so on. In a society that successfully maintains internal order, the more egregious crimes occur less frequently and typically less predictably than minor crimes. For example, murder is an extraordinary event in any society that successfully maintains a baseline of internal order; theft, however, is a much less extraordinary event, as are "victimless" crimes such as public drunkenness or prostitution.

2. Real-World Model

As strategies for ensuring internal order evolved, the four characteristics of real-world crime discussed above became embedded assumptions that shaped the traditional model of law enforcement. Proximity contributed a presumed dynamic: 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. The dynamic reflects a time when crime was parochial –

when victims and perpetrators tended to live in the same village or neighborhood.[48] Even if a victim and perpetrator did not know each other, they were likely to share community ties. This facilitated the process of apprehending perpetrators, since it was likely that a perpetrator could be identified by the victim, by witnesses or by reputation.[49] If a perpetrator and a victim did not share community ties – that is, if the perpetrator was a stranger – being an alien would no doubt contribute to his apprehension because it would be clear he "did not belong" and was therefore not to be trusted.[50] Law enforcement dealt effectively with this type of crime because its spatial limitations allowed for investigations to be limited in scope. The real-world model still assumes that the investigation of a crime should focus on the physical scene of the crime. [51]

Scale added another element: The model assumes both one-to-one victimization and the extraordinary nature of crimes, i.e., that crime is unusual and law-abiding conduct is the norm. Together, these assumptions yield the proposition that the scale of crime will be limited in a functioning society.[52] The latter assumption derives not from the physical characteristics of real-world crime but from the need to maintain internal order. A society's constitutive and proscriptive rules work together to achieve this: The constitutive rules define encouraged

---

[48]*See, e.g.,* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace, supra* note 45.

[49]*See id.*

[50]*See id.*

[51]*See id.* See, e.g., Steven A. Egger, Linkage Blindness: A Systemic Myopia, in 8 Serial Murder: An Elusive Phenomenon 163, 164 (1990).

In a stranger-to-stranger murder lacking in physical evidence or witnesses, criminal investigators are left to deal with a very large set of suspects, with only a small probability of this set including the offender.... [M]ost serial murderers are caught by chance or coincidence.... Law enforcement agencies today are simply not adept at identifying or apprehending the murderer who kills strangers and moves from jurisdiction to jurisdiction and crosses state lines.

[52]This is, of course, true. *See, e.g.,* Federal Bureau of Investigation, Crime in the United States 2002: Uniform Crime Reports 9-11 (2002), http://www.fbi.gov/ucr/cius_02/pdf/0front.pdf.

behaviors while the proscriptive rules define behaviors that will not be tolerated.[53] The members of a society are socialized to believe in and accept the constitutive rules as prescribing the "correct" standards of behavior; the proscriptive rules, or criminal laws, reinforce this by emphasizing that the behaviors they condemn are not only "bad," but fall outside the norm – they are extraordinary.[54] The combined effect of these rules is that crime becomes a subset of the total behaviors in a society; the limited incidence of criminal behavior, coupled with one-to-one victimization as the default crime mode, permits law enforcement personnel to focus their efforts on a limited segment of the conduct within a given society.[55]

The third characteristic – the physical constraints that apply to real-world crime -- structures the way the model approaches the investigation of real-world crime and the way legal systems parse responsibility for those who commit real-world crime. As to the former, the existence of physical constraints means it is appropriate to focus, at least initially, on the crime "scene," in hopes of finding witnesses who can identify the perpetrator or of finding trace evidence that can be used to identify the perpetrator.[56] As to the latter, the assumption that crime is subject to physical constraints underlies our conception of criminal jurisdiction; while jurisdiction has expanded somewhat over the centuries, the usual basis is still that the crime was "committed in" a specific, territorially-based jurisdiction.[57]

Finally, the model incorporates the concept that crime falls into identifiable patterns; this contributes to the notion that a quantum of crime is localized. The model assumes that crime

[53]*See* Brenner, *Distributed Security*, *supra* note 3.

[54]*See id.*

[55]*See id.*

[56]*See, e.g.,* Marilyn B. Peterson, Applications in Criminal Analysis: A Sourcebook 90-91 (1994).

[57]*See, e.g.,* Nev. Rev. Stat. §171.0101.

will be limited in incidence and in the types of "harm" it inflicts; it also assumes that an identifiable percentage of crime will occur in geographically and demographically demarcated areas. The combined effects of localized crime and the differential frequency with which various crimes are committed gives law enforcement agencies the ability to concentrate their resources in areas where crime is most likely to occur, thus enhancing their ability to react to completed crimes.

3. Cybercrime

Cybercrime does not require physical proximity between victim and perpetrator. Cybercrime is unbounded crime; the victim and perpetrator can be in different cities, states, or countries.[58] A perpetrator needs only a computer linked to the Internet to attack a victim's computer, to defraud someone, or to obtain the information that will allow her to assume a victim's identity and commit fraud on a grand scale.

Nor is one-to-one victimization a viable default assumption for cybercrime. One-to-one victimization is a function of the constraints that exist in the real-world; since cybercrime is not committed in that world, it is not subject to those constraints. Indeed, cybercrime does not have to involve personal victimization. Unlike real-world crime, cybercrime can be automated crime, which uses technology to carry out the commission of crimes, in whole or in part.[59] Automation allows a perpetrator to commit thousands of crimes quickly and with little effort, making one-to-

[58] *See, e.g.*, President's Working Group On Unlawful Conduct On The Internet, The Electronic Frontier: The Challenge Of Unlawful Conduct Involving The Use Of The Internet, § II(D)(2) (March, 2000), http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#CHALLENGES.

[59] *See, e.g.*, Donn Parker, *Automated Crime*, WindowSecurity.com (October 16, 2002), http://secinf.net/misc/Automated_Crime_.html/. For an example of how automation can increase the scale of criminal activity, *see, e.g.*, Kelli Arena, *U.S. Targets Porn Site's Customers*, CNN.com (August 8, 2001), http://www.cnn.com/2001/LAW/08/08/ashcroft.childporn/ (website offering child pornography had 250,000 subscribers around the world and took in $1.4 million in a one-month period).

many victimization a realistic default assumption for cybercrime.[60] This capacity for automation creates problems for law enforcement. Under the traditional model, officers react to a crime by investigating, identifying, and apprehending the perpetrator, who will be convicted and sanctioned. This scenario assumes real-world crime, that is, it assumes that crime is committed on a limited, manageable scale and can therefore be addressed by having law enforcement officers react to individual crimes. Cybercrime violates this assumption in two ways. First, even though cybercrime, like real-world crime, is carried out by a small percentage of the population of a society (or of the world, since cybercrime tends to make system boundaries irrelevant), 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.[61] As a result, the absolute scale of cybercrime, in terms of the incidence of discrete crimes, exponentially exceeds that of real-world crime. Second, cybercrime is compounded with

---

[60] *See, e.g.*, Bernhard Warner, *Cyber Blackmail Wave Targets Office Workers*, Computerworld (December 29, 2003), http://www.computerworld.com/securitytopics/security/cybercrime/story/ 0,10801,88623,00.html:

> The extortion scam . . . targets anyone on the corporate ladder with a PC connected to the Internet. It . . . starts with a threatening e-mail in which the author claims to have the power to take over a worker's computer . . . . The e-mail typically contains a demand that unless a small fee is paid . . . the fraudster will attack the PC with a file-wiping program or download onto the machine images of child pornography.
>
> 'They prey on the nice secretary . . . . When she gets one of these e-mails, she . . . puts it on her credit card and transfers the funds . . . and hopes it goes away,' a British detective specializing in cybercrime told Reuters . . . . There are scores of cases of companies . . . receiving extortion threats . . . . Fraudsters also send out streams of menacing e-mails with hollow threats of cyber sabotage. The scam works even if only a handful of the countless recipients pay up.
>
> `It's getting simpler,' said [F-Secure's Mikko] Hypponen. `If you wanted to extort money from a small company, you would have had to hack them and convince them you have stolen their information. Here, you don't have to do anything but send an e-mail around.'

[61] *See, e.g.*, President's Working Group On Unlawful Conduct On The Internet, The Electronic Frontier, *supra* note 58 ("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 . . . in the offline world").

the real-world crime with which law enforcement has traditionally dealt and with which it must continue to deal; people will, after all, continue to rape, rob, and murder in the real-world. These factors combine to cause an overload for the traditional model: Law enforcement's ability to react to cybercrime erodes because the resources that were barely adequate to deal with real-world crime are totally inadequate to deal with cybercrime and with cybercrime-plus-real-world-crime.

Cybercrime perpetrators avoid the physical constraints that govern real-world crime. A cybercrime can be committed instantaneously. For example, a virtual bank robbery can be committed and the funds can be deposited into accounts in several other countries before law enforcement learns that the crime has been committed. Law enforcement's reactive strategy is considerably less effective in this context than in the real-world.[62] For one thing, the reaction begins well after the crime has been successfully concluded. Since all or substantially all of the conduct involved in committing the crime occurs in an electronic environment, the "physical" evidence, if any, is evanescent and volatile. By the time officers react to the robbery, any electronic evidence that existed may well have been destroyed, advertently or inadvertently. Also problematic is that the perpetrator was never physically present at the crime scene; thus, assumptions about his having been observed in the processes of preparing for, committing, and/or fleeing from the crime no longer hold. It may be impossible for officers to determine the identity of the perpetrator or the physical location from which he carried out this crime; unlike the real-world perpetrators, cybercriminals can take advantage of perfect anonymity or perfect

[62]See, *e.g., FBI Overwhelmed By Cybercrime,* Reuters (March 20, 2002), http://zdnet.com.com/2100-1105-864453.html.

pseudonymity.[63] Even if officers can identify the perpetrator, gathering evidence and apprehending him can be difficult, since the country that hosts the perpetrator may not regard his actions as illegal. The host country may therefore decline to extradite him, or there may be no extradition treaty in place that governs the conduct at issue.[64]

Finally, perhaps because cybercrime is still a new phenomenon, we are unable to identify offender-offense patterns comparable to those for real-world crime; as a result, law enforcement cannot effectively allocate its resources to deal with real-world crime. Several factors account for our inability to identify cybercrime patterns.[65] First, they are not accurately documented. Countries do not track cybercrime the way they track real-world crime, perhaps because of a lack of standardized definitions of cybercrime.[66] While law enforcement agencies record cybercrimes, they tend not to break them out into a separate category; cyberfraud, for example, is recorded as "fraud."[67] Additionally, it can be difficult to parse cybercrime into discrete offenses: Was the "Love Bug" virus that caused billions of dollars of damage in more than twenty countries one crime or thousands of crimes? Clearly, though, the most important reasons for our

---

[63]*See, e.g.*, David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 11 U. Chi. Legal F. 139, 149-51 (1996).

[64]*See, e.g.*, Susan W. Brenner & Joseph Schwerha IV, *Transnational Evidence-Gathering and Local Prosecution of International Cybercrime***,** 20 J. Marshall J. Computer & Info. Law 347, 375-377 (2002).

[65]It may be that cybercrime, unlike real-world crime, does not fall into identifiable patterns. *See* Brenner, *Distributed Security*, *supra* note 3.

[66]*See, e.g.*, Barbara Etter, Critical Issues in High-Tech Crime, Australasian Centre for Policing Research 9 (2002), http://www.acpr.gov.au/pdf/Presentations/CIinHi-tech.pdf.

[67]*See, e.g.*, Federal Bureau of Investigation, Uniform Crime Reports 2002, http://www.fbi.gov/ucr/cius_02/02prelimannual.pdf. *But see* Bureau of Criminal Justice Statistics, Prosecutors in State Courts 2001 5 (May 2002), http://www.ojp.usdoj.gov/bjs/pub/pdf/psc01.pdf (reporting number and type of cybercrime prosecutors by state prosecutors). Cybercrime statistics are complied in a few specialized areas. *See, e.g.*, Internet Fraud Complaint Center, IFCC Annual Internet Fraud Report 2002, http://www1.ifccfbi.gov/strategy/statistics.asp.

lack of accurate statistics about cybercrime are that (i) many cybercrimes go undetected and (ii) many detected cybercrimes go unreported. As to the first issue, cybercrime often goes undetected either because security systems cannot detect outside penetrations or because they are carried out by trusted insiders, who know how to hide their tracks.[68] As to the second issue, commercial victims are notorious for not reporting that they have been victimized by a cybercriminal. These companies do not want to advertise their vulnerability, either to customers or to their shareholders.[69]

4. Cybercrime Model

The current model of law enforcement was in place by the first quarter of the nineteenth century, a period when technology was in its infancy. The traditional model of law enforcement is in many respects analogous to the traditional model of military order: Both are concerned with organizing and concentrating human and other forces to respond to physical activity, or the prospect of such activity, by human beings who are situated in an identifiable physical environment. Both models therefore feature a hierarchical structure that uses a chain of command to concentrate personnel and other resources on those to whom a response is necessary; this is an appropriate approach to concentrating human and other resources to achieve an objective in the real-world, which is why both models survived for so long.[70]

---

[68] *See, e.g.,* Andrew P. Snow & Mark Longworth, *The Greatest Information Survivability Threat: The Undetected Barbarian at the Gates*, CERT: Fourth Information Survivability Workshop (2001), *at* http://www.cert.org/research/isw/isw2001/papers/Snow-31-08.pdf

[69] *See, e.g.*, Art Jahnke, *The GAO Assessment of the Fed's Cybercrime Unit: Hard to Tell*, Darwin Magazine (May 29, 2001), *at* http://www.darwinmag.com/connect/opinion/column.html?ArticleID=107.

[70] *See, e.g.*, Brian Nichiporuk & Carl H. Builder, *Societal Implications* in Athena's Camp: Preparing for Conflict in the Information *Age* 297 (1997), *available at* http://www.rand.org/publications/MR/ MR880/MR880.ch13.pdf ("Hierarchical organizations have been a salient characteristic of human civilization; they are the basis upon which most authority, power, and command and control have been exercised for millennia").

Technology eliminates the need, and indeed the ability, to focus on specific, localized activity. Communication technologies free us from the constraints of the empirical world; we can communicate instantaneously with anyone from anywhere.[71] This produces a new type of social organization: the network.[72] The emergence of the network is not without precedent; the development of new technologies has historically produced new forms of social organization.[73] Networks are displacing hierarchies in every sector of society, including the military, because hierarchical organization is not an effective means of organizing technologically-mediated activities.[74]

Networks are lateral, fluid systems;[75] they decentralize power and authority, thereby empowering individuals.[76] While networks have the capacity to usher in a new era of cooperation among peoples and among social systems,[77] they can also be exploited for destructive purposes:

> [T]he rise of hierarchical forms of organization . . .was . . . attended . . . by the appearance of ferocious chieftains bent on military conquest . . . . [T]he early spread of the market form . . . was accompanied by a spawn of . . . pirates, smugglers, and monopolists. . . . There appears to be a subtle . . . interplay between the bright and dark sides in the rise of a new form of organization. The bright-side actors may be so deeply embedded in and constrained by a society's established forms of organization that many have difficulty becoming the . . .

---

[71] *See, e.g.*, Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, 4 N.C. J. L. & TECH. 1, 25 (2002), *at* http://www.jolt.unc.edu/.

[72] *See, e.g.*, David Ronfeldt & John Arquilla, *Networks, Netwars and the Fight for the Future*, 6 First Monday, (October 2001), *at* http://firstmonday.org/issues/issue6_10/ronfeldt/index.html.

[73] *See, e.g.*, David Ronfeldt, *Tribes, Institutions, Markets, Networks: A Framework About Social Evolution* 5-17 RAND (1996), *available at* http://www.rand.org/publications/P/P7967/P7967.pdf.

[74] *See* Nichiporuk & Builder, *supra* note 70, at 298-299. *See also* John Arquilla & David Ronfeldt, *Swarming & The Future of Conflict* 1-10 (2000), *available at* http://www.rand.org/publications/DB/ DB311/DB311.pdf.

[75] *See id.*

[76] *See id.*

[77] *See, e.g.*, HOWARD RHEINGOLD, SMART MOBS: THE NEXT SOCIAL REVOLUTION 208-251 (2002) ("cooperation amplification").

> adopters of a new form. In contrast, nimble bad guys may have a freer, easier time acting as the cutting edge. . . .[78]

This is precisely what is occurring as to cybercrime. Law enforcement, which is for the most part still "embedded in and constrained by" traditional hierarchy, lags behind the "bad guys" who have learned how to exploit the distributed, non-territorially-based realities of cyberspace. Thus, the question becomes: How do we bring law enforcement up to speed and how can law enforcement adapt to the new realities of cybercrime?

The core problem is evident in law enforcement's reactive approach. As Part II(A)(3) demonstrated, the reactive approach does not effectively deal with cybercrime, since cybercrime is not territorially based and tends therefore to be elusive. There is no necessary nexus between the situs of a cybercrime and the perpetrator's physical location, either at the time the crime is committed or afterward; no one observes the perpetrator casing the crime scene, "traveling" to it, committing the crime or "fleeing" the scene. Cybercriminals can shield their identities and do not leave traditional physical evidence at the crime scene; whatever evidence they leave can easily be lost, destroyed or altered. Cybercrimes do not fall into identifiable patterns and the scale of their commission means law enforcement officers simply cannot react to all of them.

One solution would be to improve law enforcement's ability to react to cybercrimes. This could involve taking any of several actions. First, the number of officers who are available to react to cybercrime could be significantly expanded. As Part II(A)(3) noted, cybercrime is problematic for law enforcement because it constitutes an incremental addition to the quantum of crime to which law enforcement must react; thus, it seems logical that increasing the number of officers available to react should offset this effect and restore the efficacy of the reactive

[78]David Ronfeldt & John Arquilla, *What Next for Networks and Netwars?* In Networks and Netwars: The Future of Terror, Crime and Militancy 313 (John Arquilla & David Ronfeldt eds. 2001), *available at* http://www.rand.org/publications/MR/MR1382/MR1382.ch10.pdf .

strategy. There are, unfortunately, two problems with this solution. First, societies already find it difficult to allocate the resources necessary to support existing law enforcement agencies; therefore, it is highly improbable that they will be able to summon the resources required to recruit, train and equip enough officers to make the reactive strategy a viable approach to cybercrime. Additionally, since cybercrime is, and will continue to be, increasingly automated, there is no guarantee that increasing the number of officers will improve the efficacy with which law enforcement agencies can react to cybercrime. It is no longer a matter of fielding officers to track down and apprehend a perpetrator before he can re-offend; while officers are searching for the perpetrator of one cybercrime, the same perpetrator can use his automated systems to commit hundreds or even thousands of other crimes[79] to which officers will also have to react. Furthermore, as was illustrated in Part II(A)(3) , it is difficult for officers to react effectively even when they are available to do so; they may never find the perpetrator and, if they do, they may not be able to arrest, prosecute, or convict him.

Another alternative would be to fight fire with fire: to automate policing in cyberspace. This would presumably involve using automated agents to react to completed cybercrime and to "patrol" public areas of cyberspace in an effort to apprehend cybercriminals in much the same way state troopers patrol interstate highways and apprehend speeders. While automated cyberpolicing is a logical alternative, its adoption and implementation would be fraught with difficulties, technical and legal, [80] that make it an unrealistic option for the foreseeable future.

---

[79]*See, e.g.*, Testimony of Alan Paller, Director of Research – The SANS Institute, Before the U.S. Senate Committee on Governmental Affairs, Hearing on "Securing Our Infrastructure: Private/Public Information Sharing" (May 8, 2002), *at* http://www.senate.gov/~gov_affairs/050802paller.pdf ("The fight against cybercrime resembles an arms race where each time the defenders build a new wall, the attackers create new tools to scale the wall").

[80]*See, e.g.*, Kevin Manson, *Robots, Wanderers, Spiders and Avatars: The Virtual Investigator and Community Policing behind the Thin Digital Blue Line*, Office of International Criminal Justice (1997), *at*

Yet another possible solution is to authorize civilian use of defensive technologies which would let cybercrime victims use "strike-back" or "counterstrike tools".[81] Victims could react when they become the targets of cybercrime and would supplement the reactive capabilities of law enforcement personnel.[82] Like the automated cyberpolicing strategy, this alternative raises difficult legal questions.[83] The risks involved in authorizing victim self-help, however, would ultimately cause this approach to founder. Tracing a cyberattack to the perpetrator's computer may be impossible for victims with limited technical skills;[84] consequently, they may "retaliate" against the wrong computer system. Since many systems are "operated by hospitals, governmental units, and telecommunications entities . . . that provide connectivity to millions of people," counterstrikes such as these "could easily create a remedy worse than the disease."[85]

These alternatives exhaust the options for improving the reactive approach, so it seems we must devise a new approach. There are two ways of logically dealing with crime: reacting to completed crimes and preventing crimes before they are committed. The reactive model incorporates the concept of crime prevention insofar as it is predicated on incapacitating and deterring offenders, but this is not its primary concern.[86] Preventing crime is the primary concern of another model: "community policing." Community policing emphasizes "putting

---

http://www.dougmoran.com/tatzlwyrm/CACHE/Digital_Officer_Safety/Attachments/Robots_Wanderers_Spiders_and_Avatars.PDF ("Matters of comity, sovereignty and legal jurisdiction will . . . have to be resolved before intelligent agents begin coursing through servers in foreign universities, banks and government agencies").

[81]Curtis E.A. Karnow, *Strike and Counterstrike: The Law on Automated Intrusions and Striking Back*, Black Hat Windows Security (February 27, 2003), *at* http://www.blackhat.com/presentations/win-usa-03/bh-win-03-karnow-notes.pdf.

[82]*See id.*

[83]*See id. (*"A host of statutes . . . make it illegal to attack or disable computers, including those connected to the Internet").

[84]*See id.*

[85]*Id.*

[86]*See supra* Part II(A)(2). *See also supra* Part I.

officers back on the streets," where they become "part of the fabric of the neighborhood, as a . . . dependable presence, instead of racing around the city in patrol cars, reacting to crimes that have already happened."[87] It also emphasizes cooperation between police and citizens to create a climate where crime is not tolerated.[88] Community policing has had notable successes in the real-world, but it is difficult to implement, since it is labor-intensive, requires organizational restructuring, and can raise ethical issues about the allocation of scarce resources.[89]

Community policing, as such, is not a viable option for the cyber-world for two reasons. First, it would require assigning police officers to "patrol" cyberspace; it would therefore be necessary to staff these patrols either by hiring new officers or re-assigning officers who deal with real-world crime to cyberspace.[90] The first option would require funds that, as was explained earlier, are simply not available. The second would erode the law enforcement presence in the real-world in order to concentrate on cybercrime; since real-world crime poses its

---

[87]Lancaster (Pa.) Crime Commission, Crime Commission Report 2003 § II ("Community Policing and Law Enforcement Organization"), *at* http://www.lancasteronline.com/crimereport/0302/comm_police.shtm. *See, e.g.*, Lawrence Sherman, *Preventing Crime: What Works, What Doesn't, What's Promising*, A Report to the United States Congress for the National Institute of Justice (1997), *at* http://www.ncjrs.org/works/.

[88]*See* Lancaster Crime Commission, Crime Commission Report 2003, *supra* note 87. *See also* Barry N. Leighton, *Visions of Community Policing: Rhetoric and Reality in Canada*, 33 CANADIAN J. CRIMINOLOGY 485, 487 (1991).

[89]*See, e.g.*, Leighton, *supra* note 88, at 496-498, 503-511; David Thacher, *Equity and Community Policing: A New View of Community Partnerships*, 20 CRIM. JUSTICE ETHICS 1 (2003); Gerasimos A. Gianakis & G. John Davis III, *Reinventing or Repackaging Public Services? The Case of Community-Oriented Policing*, 58 PUB. ADMIN. REV. 1 (1998).

[90]Many agencies have officers who are assigned to cyber crime, and many of them "patrol" areas of cyberspace. None, however, maintains a 24/7 presence in cyberspace and it is exceedingly unlikely that any will be able to do so in the foreseeable future. *See, e.g.*, Gary Nurenberg, *Cracking Down on Online Predators* (Tech TV television broadcast, Aug. 27, 2002) *available at* http://www.g4techtv.com/techtvvault/features/28652/Cracking_Down_on_Online_Predators.html (last visited Sept. 22 2004); Molly Masland, *Stalking Child Molesters on the Net* (MSNBC television broadcast Sept. 4, 1998) *at* http://msnbc.msn.com/id/3078773/.

own compelling dangers, this would not be advisable. Further, community policing is not a viable option for the cyber-world because there really are no "communities" in cyberspace. "Communities" in cyberspace tend to be defined by interests, not by territory.[91] In the real-world, community policing succeeds because the civilians who participate want to ensure the security of the neighborhood in which they live. In the cyber-world, the members of these interest-based "communities" may not be concerned about cybercrime because they lack the central, binding focus that a physical neighborhood provides. Considering the interests and communications that give rise to these communities, many of the participants may prefer the risk of cybercrime to the prospect of a law enforcement presence in their midst.

While this form of community policing cannot be applied to cyberspace, two aspects of the community policing model suggest an approach that could be used for cybercrime: proactivity and collaboration. The reactive model of law enforcement does not deal effectively with cybercrime because it is fluid and distributed in nature. Thus, as a lateral, pervasive phenomenon, cybercrime requires a lateral, pervasive solution. This solution must be proactive; that is, it must focus on preventing cybercrime because, as explained above, reacting to completed crimes is not a practicable means of dealing with cybercrime. The solution must also involve a collaborative approach that combines the efforts of civilians and law enforcement in order to address the fact that it is neither financially nor pragmatically possible to deploy enough officers to maintain order in cyberspace. Clearly, then, a practical way to address cybercrime is to utilize the community policing model's concept of a proactive, collaborative approach to preventing crime.

---

[91] *See* Peter Kollock & Marc A. Smith, *Communities in Cyberspace*, *in* COMMUNITIES IN CYBERSPACE 3-28 (Marc A. Smith & Peter Kollock eds., 1998). *See, e.g.*, *Welcome to Communities.com at* http://www.communities.com/ (last visited Sept. 22, 2004).

How is this to be done? Does this solution require creating yet another model of law enforcement, one specifically directed at cybercrime? Actually, this solution does not require a new model as much as it requires eliminating the assumptions and expectations that are the foundation of the traditional model and replacing them with a new set of assumptions and expectations. Under the traditional model, citizens have no responsibility for dealing with crime; they have come to think of crime as the exclusive responsibility of the police.[92] The community policing model seeks to reverse this process, at least in part, and to involve citizens in combating crime.[93] It achieves this by putting officers in neighborhoods where they patrol the area to discourage criminal activity and encourage citizens not to tolerate such activity. Citizens are involved, but only in preventing crime; they are not responsible for reacting to it.[94]

This community policing model is ineffective against cybercrime, however, because police cannot patrol "neighborhoods" in cyberspace. The model relies on an active police presence, reinforced by neighborhood support, to control crime in a specific geographical location. It cannot be applied in a context that lacks geography and neighborhoods.

[92]*See, e.g.*, William D. Eggers & John O'Leary, *The Beat Generation: Community Policing at Its Best*, 74 Pol'y Rev. 1 (1995), *available at* http://www.policyreview.org/fall95/thegg.html ("The public began to forget its role in controlling crime and grew increasingly dependent on the police . . . . Americans began to think of crime fighting as the job of police."). *See also* Richard A. Leo, *Some Thoughts about Police and Crime* in THE CRIME CONUNDRUM, ESSAYS ON CRIMINAL JUSTICE 121 (George Fisher & Lawrence M. Friedman eds., 1997).

[93]Prior to the rise of the traditional model, citizens were involved in law enforcement; indeed, for much of modern history, citizens *were* law enforcement. In 1285, for example, the English Statute of Winchester established a system of patrols in the "large towns of England. Men between the ages of fifteen and sixty were required to perform watch service . . . . They were responsible for . . . apprehending anyone who committed a crime." CYRIL D. ROBINSON, RICHARD SCAGLION & J. MICHAEL OLIVERO, POLICE IN CONTRADICTION : THE EVOLUTION OF THE POLICE FUNCTION IN SOCIETY 20 (1994). The statute also "required every man between the ages of fifteen and sixty to maintain specified weaponry, which varied according to his wealth." David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1197 (1999). For the transition from citizen law enforcement to professional law enforcement under the traditional model see Brenner, *supra* note 3, *Distributed Security*.

[94]*See, e.g.*, Brenner, *supra* note 3 *Distributed Security*.

Nevertheless, a variation of the model could be used to prevent cybercrime. This modified community policing model relies primarily on active citizen efforts and only secondarily on police support. This is not a *community* policing model; it is a *distributed* policing model in which citizens assume responsibility for preventing crime. This modified community policing model represents the disassembling of the traditional model of law enforcement insofar as citizens assume responsibilities with regard to a particular type of crime, e.g., burglary;[95] their responsibilities consist primarily of preventing cybercrime, though citizens may also be encouraged to report cybercrimes to law enforcement.[96] Citizen prevention serves to maintain internal order; it also serves to ward off external threats because cyberattacks, unlike real-world crimes, can constitute acts of terrorism or war.[97]

Postulating this model raises two questions: Why should citizens assume responsibility for preventing cybercrimes when they have no such responsibility as to real-world crimes? Assuming citizens should assume such responsibility, how can this be achieved? Both questions are addressed below.

(a) Why?

The answer to the "why" question lies in the differences between cybercrime and real-world crime. We do not require citizens to prevent real-world crimes. For example, assume that I go work and leave my front door unlocked and a rear window wide open. If a burglar takes advantage of the situation and steals my television, my laptop, and my stereo, I can call the

[95]As explained above, it also represents a return to an older approach, the approach that anteceded the quasi-military, hierarchical model of professional law enforcement that has been the norm for just over a century. *See supra* note 93.

[96]As was explained earlier, it is not advisable to hold civilians responsible for reacting to completed cybercrime. *See supra* notes 81-85 and accompanying text.

[97]*See, e.g.*, OFFICE OF THE PRESIDENT, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 5-7, 37-41 (February 2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf. *See also infra* note 108.

police, who will make an effort to find the burglar and recover my property. It is, of course, quite possible that the officers may not exert themselves to the fullest in doing so; they may make the burglary of my home a lesser priority than other crimes out of their frustration at my irresponsibility. I, however, will never know if this is the case and, indeed, it may not be; the officers may well make a sincere effort to recover my property and apprehend the perpetrator. My irresponsibility is legally irrelevant; criminal law does not require a blameless victim. It is a crime to inflict a prohibited harm on an individual even though he recklessly exposed himself to the risk of such harm or consented to its infliction.[98] The doctrinal reason why the criminal law disregards my carelessness is that a crime is an offense against the authority of the state and therefore must be addressed by the state without regard to the circumstances that contributed to its commission.[99] This proposition derives from the systemic need to maintain internal order and the empirical reality that criminal behavior constitutes a serious threat to such order.[100]

Why should citizen obligations be different with regard to cybercrime? The primary reason is that if I leave my front door unlocked and a rear window open and a burglar takes advantage of my carelessness, the only one harmed is me, the architect of my own victimization. This is not necessarily true for cybercrime. Assume that instead of leaving my front door unlocked and a rear window open, I access the Internet using an always-on broadband connection without installing any security software to prevent my computer from being hijacked by a hacker. I have opened my computer up to attack, which creates a situation analogous to the

[98]*See, e.g.*, Commonwealth v. Atencio, 345 Mass. 627, 189 N.E.2d 223 (Mass. 1963) (state had an interest in seeing that the victim, who died while playing Russian roulette, "should not be killed by the wanton or reckless conduct of himself or others"). *See also* Commonwealth ex rel. Smith v. Myers, 438 Pa. 218, 234-235, 261 A.2d 550, 558 (Pa. 1970) (`a killing with the victim's consent is nevertheless murder'") (quoting Case Note, 71 Harv. L. Rev. 1565 (1958)).

[99]*See, e.g.*, Commonwealth v. Atencio, *supra*, 345 Mass. 627, 189 N.E.2d 223 (Mass. 1963).

[100]*See supra* Part I.

burglary scenario: I have carelessly exposed myself to "harm" from a criminal. However, I have also created the potential for "harm" to others. My carelessness has created a situation in which a hacker can take over my computer and use it to victimize other individuals and entities.[101] This scenario results in the infliction of incremental "harms" exceeding those I would suffer from a personal attack. A cybercriminal can use my computer, along with other hijacked computers, to launch a denial of service attack on an online business or a government website and shut them down; to do this, the perpetrator requires access to a critical mass of zombie computers,[102] which I have helped to supply.[103] The effects of my carelessness will be particularly egregious if terrorists or organized criminals use my computer to attack my country's infrastructure;[104] it is at this point that victim defaults jeopardize a system's ability to sustain internal and external order.[105] Thus, the most compelling answer to the "why" question is that responsibility for preventing cybercrimes should be imposed upon citizens because their failure to secure their own systems can result in the infliction of "harm" upon others, potentially threatening the security of the entire system.[106]

Another justification for requiring greater citizen responsibility is that law enforcement is less effective in maintaining order in cyberspace than in the real-world. In the real-world

---

[101] *See, e.g.*, Bob Sullivan, *Could Your Computer be a Criminal?*, MSNBC *at* http://www.msnbc.com/news/939227.asp (July 15, 2003). *See also* OFFICE OF THE PRESIDENT, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 39 (February 2003), *available at* http://www.whitehouse.gov/pcipb /cyberspace_strategy.pdf; Brenner, *supra* note 3 *Distributed Security*.

[102] A zombie computer is a "computer containing a hidden software program that enables the machine to be controlled remotely, usually to perform an attack on another computer". Word Spy, "Zombie Computer," http://www.wordspy.com/words/zombiecomputer.asp.

[103] *See, e.g.*, Xianjun Geng & Andrew B. Whinston, *Defeating Distributed Denial of Service Attacks*, *available at* http://cism.bus.utexas.edu/works/articles/defeating_ddos.pdf (August 2000).

[104] *See infra* note 383 & accompanying text.

[105] *See supra* Part I. *See also* Brenner, *Distributed Security*, *supra* note 3.

[106] *See, e.g.*, OFFICE OF THE PRESIDENT, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 101, at 5-8.

scenario, police may well apprehend the burglar who stole my property; he may have been seen by my neighbors, left trace evidence in my house, or brought attention to himself when he tried to dispose of the property he took from me. In the cyber-world example, the cyberperpetrator stands an excellent chance of avoiding apprehension because he acts remotely and anonymously and does not leave a trail in the physical world.[107] Since citizen lapses in security can endanger others and since law enforcement cannot itself maintain order in cyberspace, it is prudent and reasonable for citizens to assume a measure of responsibility for maintaining order.[108]

(b) How?

Assuming citizens should undertake such an obligation, we must now consider *how* citizens are to become responsible for preventing cybercrime. There are two alternatives: through voluntary or obligatory conduct. Voluntary conduct is conduct individuals engage in because they believe it is "right" or "appropriate."[109] Individuals' belief that particular conduct is "right" or "appropriate" (and, conversely, that other conduct is "wrong" or "inappropriate") is

---

[107] *See supra* Parts II(A)(3)-(4).

[108] *See supra* note 93. This issue is also addressed in Part II(B), *infra.* Requiring that citizens assume such responsibility promotes external order as well as internal order because cyberattacks can represent information warfare or cyberterrorism, as well as cyber crime. *See, e.g.*, OFFICE OF THE PRESIDENT, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 101, at 7:

> In the last century, geographic isolation helped protect the United States from a direct physical invasion. In cyberspace national boundaries have little meaning . . . . Even the infrastructure that makes up cyberspace . . . is global in its design and development. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them.

Countries can launch surreptitious yet effective attacks via cyberspace, exploiting security lapses on the part of civilians, and terrorists can do precisely the same thing. *See id.* ("the computers of home users can become part of networks of remotely controlled machines . . . used to attack critical infrastructures").

[109] *See, e.g.*, Richard H. McAdams, *An Attitudinal Theory of Expressive Law*, 79 OR. L. REV. 339, 340-349 (2000); Paul H. Robinson & John M. Darley, *The Utility of Desert*, 91 Nw. U. L. REV. 453, 469-471 (1997).

based on norms they have internalized; voluntary conduct is therefore the product of internal social control mechanisms.[110] Obligatory conduct, on the other hand, is the product of external social control mechanisms.[111] It is conduct individuals engage in or avoid engaging in because they know that their failure to conform to what is externally required can result in their being sanctioned by that system.[112]

A voluntary approach to achieving citizen responsibility for preventing cybercrime would require establishing a norm to that effect; once the members of a society internalize this norm, they would regard preventing cybercrime as the "right" or "appropriate" thing to do, and most individuals would endeavor to comply. [113] Creating such a norm would require educating the populace in the need to take preventative efforts and in the means of implementing such efforts.[114] Ideally, a voluntary approach is the preferred option; the most effective means of channeling behavior into desired paths is not the "imposition of external sanction**,** but the inculcation of internal obedience."[115] Unfortunately, establishing a norm can take a very long time.[116] This is likely to be particularly true with regard to cybercrime prevention because the norm to be created involves cyberspace, and cyberspace is still an alien environment for most

---

[110]*See infra* Part II(B).

[111]*See id.*

[112] Obligatory conduct is voluntary in the sense that a member of a social system decides whether she will engage in the prescribed conduct; it is not "voluntary" in the sense used above because the decision to behave in particular ways is prompted by the awareness of externally-imposed consequences for one's failure to do so. *See id.*

[113]*See e.g.*, McAdams, *supra* note 106, at 340-49; Robinson & Darley, *supra* note 106, at 453, 469-71.

[114] It might also include appeals to their sense of system loyalty by emphasizing the impact cybercrime can have upon a system's economy and the potential for external threats to system infrastructures. *See supra* Part II(A)(4).

[115]Harold Hongju Koh, *How Is International Human Rights Law Enforced?*, 74 IND. L.J. 1397, 1401 (1999)*; see, e.g.*, TOM R. TYLER, WHY PEOPLE OBEY THE LAW 4 (1990).

[116]*See generally* Richard A. Posner & Eric B. Rasmussen, *Creating and Enforcing Norms with Special Reference to Sanctions*, 19 INT'L REV. L. & ECON. 369, 377-80 (1999).

people.[117] Citizens may believe it is prudent to install alarms and "burglar bars" to ward off real-world threats, but most are unlikely to appreciate the dangers that can come from cyberspace. Further, the difficulty of creating such a norm is exacerbated by the fact that it would have to at least partially displace a deeply embedded norm, i.e., the idea that dealing with crime is the exclusive province of law enforcement.[118] For these reasons, and others, a purely voluntary approach is unlikely to be effective, at least not in the near future.

This leaves the obligatory approach, which requires citizens to behave in certain ways. They can be required to act or not to act, [119] and the law is used to establish such an obligation.[120] "Do" laws create an obligation to act and impose sanctions for failing to discharge that obligation;[121] "do not" laws create an obligation not to act and impose sanctions for committing the proscribed act.[122] Though civil or criminal laws can be used to implement an obligatory approach, this discussion assumes criminal liability is used to impose an obligation to prevent cybercrime. Criminal liability is generally more effective than civil liability in encouraging citizens to conform their conduct to a prescribed standard.[123] The question, therefore, is whether this obligatory approach should utilize "do" laws or "do not" laws.

---

[117] *See* Brenner, *Distributed Security*, *supra* note 3.

[118] *See supra* Part II(A)(2).

[119] *See, e.g.*, FREDERICK SCHAUER, PLAYING BY THE RULE: A PHILOSOPHICAL EXAMINATION OF RULE-BASED DECISION-MAKING IN LAW AND IN LIFE 7 (1991); *see also* H.L.A. HART, THE CONCEPT OF LAW 28 (1975).

[120] *See, e.g.*, Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 6.2 (2003).

[121] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS §§ 314A, 322 (1965); MODEL PENAL CODE § 2.01(3).

[122] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 21 (1965); MODEL PENAL CODE § 2.01(1).

[123] *See e.g.*, Robinson & Darley, *supra* note 109, at 472 ("criminal law builds and maintains societal norms in several…ways"); *see also* Geraldine Szott Moohr, *Federal Criminal Fraud and the Development of Intangible Property Rights in Information*, 2000 U. ILL. L. REV. 683, 730 (2000); Lior Jacob Strahilevitz, *how Changes in Property Regimes Influence Social Norms: Commodifying California's Carpool Lanes*, 75 IND. L.J. 1231, 1278-79 (2000).

A strategy utilizing "do" laws would impose an obligation to prevent cybercrime;[124] a failure to discharge that obligation would result in a sanction.[125] Seat belt laws provide a useful point of comparison. By 2002, forty-nine states and the District of Columbia had enacted such laws.[126] These "do" laws require the occupants of a motor vehicle to use seat belts when the vehicle is in operation and impose sanctions for failure to comply.[127] Seat belt laws have been effective in increasing seat belt use among American motorists,[128] so it might seem that a similar approach would be an effective way to impose responsibility for preventing cybercrime.

There are, however, important differences between the two types of security measures. One differentiating factor is the relative complexity of the duty being imposed. Federal law required that vehicles manufactured after 1968 have seat belts, so they were available when states began requiring their use.[129] Thus the duty imposed by seat belt laws was not an onerous one – citizens are to use a device that is available and requires no technical skill to employ. The duty imposed by the proposed cybercrime prevention laws, however, would be far more complex: Citizens would have to (i) identify and obtain the tools they need to protect their

---

[124]For individuals, this obligation could encompass installing firewalls and other security measures on computers, installing, updating and using anti-virus software and keeping software updated. *See, e.g.*, Office of the President, *supra* note 97, at 39. For artificial entities, it could include these activities along with addressing insider threats and sharing information about known threats. *See id.* at 39-41.

[125]The sanction would no doubt be a fine; restrictions on computer use might be added for intransigent violators. Such laws should be structured to alleviate or eliminate liability for attacks that could not reasonably be prevented by the measures available to average citizens. *See infra* Part II(C)(1).

[126]*See e.g.*, David A. Mobley, *Revisiting Alabama's Seat Belt Defense: Is the Failure to Buckle Up a Defense in AEMLD Claims?*, 53 ALA. L. REV. 963, 969 n.45 (2002).

[127]*See, e.g.*, CAL. VEH. CODE § 27315(d)-(i) (West 2004); MASS. GEN. LAWS ANN. ch. 90, §13A (West 2001).

[128]*See e.g.*, Barry L. Huntington, Comment, *Welcome to the Mount Rushmore State! Keep Your Arms and Legs Inside the Vehicle at All Times and Buckle Up . . . Not for Safety, but to Protect Your Constitutional Rights*, 47 S.D. L. REV. 99, 104 (2002).

[129]*See e.g.*, Mobley, *supra* note 126, at 996 (citing 23 C.F.R. § 255.21 (1968)).

computers from cybercriminals; (ii) educate themselves about these tools so they could install them, use them, keep them updated, and replace them when necessary; and (iii) use these tools in an effective manner. Since computer software, hardware, and the threats in cyberspace are all constantly evolving, these tasks would be ongoing and demanding obligations.

Another differentiating factor is the likelihood that scofflaws will be sanctioned. Both the seat belt laws and the hypothesized cybercrime prevention laws establish a duty and impose sanctions to deter what society regards as dangerous behavior. The behaviors to be deterred, respectively, are not wearing seat belts and thereby exposing oneself to a risk of injury; and not utilizing cybercrime preventative measures and thereby exposing oneself, others, and the social system to cyberattackers. The effectiveness of sanctions in deterring behavior is a function of the perceived risk of actually being apprehended and sanctioned; the deterrent effect increases as the perceived risk of apprehension increases.[130] Since compliance with seat belt laws occurs in public, it is not difficult for officers to tell if someone is obeying the law. The perceived risk of being apprehended is therefore high; that, coupled with the ease with which one can comply with the law, makes the seat belt laws an effective type of "do" law. The same would not be true for cybercrime prevention laws; these "do" laws would primarily address conduct occurring in private places – one's home or office.[131] Absent remote monitoring (which raises Fourth Amendment issues),[132] it would be difficult for those charged with enforcing such laws to determine compliance. The perceived risk of being identified and apprehended would

[130]*See e.g.*, Thomas D. Griffith, *Habitual Offender Statutes and Criminal Deterrence*, 34 CONN. L. REV. 55, 60-61 (2001).

[131]Since these laws would encompass preventative measures taken to secure laptops and other portable computing devices, it is conceivable that an officer would observe a failure to implement such measures when a laptop or other device was being used in public.

[132]*See, e.g., Kyllo v. United States*, 533 U.S. 27, 35 (2001).

consequently be low; coupled with the difficulty of complying, this means that these hypothesized "do" laws would not be an effective means of securing citizen collaboration in enhancing cybersecurity.[133]

This leaves the final option: "do not" laws. "Do not" laws may seem a peculiar candidate for enlisting citizens in the fight against cybercrime because "do not" laws generally define crimes.[134] After all, we are not talking about sanctioning citizens for *committing* cybercrime; we are talking about sanctioning them for failing to *prevent* cybercrime.

Actually, "do not" laws should serve quite nicely. One problem with using "do" laws is that such an approach is fundamentally inconsistent with how we approach criminal liability. Under the approach outlined above,[135] we impose a duty on citizens to prevent their becoming victims of cybercrime and we sanction them if they fail to do so. This is inconsistent with how we approach criminal liability because (i) it imposes an unprecedented obligation to prevent crime;[136] and (ii) it imposes criminal liability for failing to discharge this obligation *even though*

[133]"Do" laws of the type hypothesized might very well be perceived as Draconian, intrusive and, given the public lack of awareness of the dangers of cybercrime, unnecessary; such perceptions could result in widespread disregard of the obligation to be imposed, just as the alcohol Prohibition laws of the 1920's were met with resistance. *See* Brenner, *Distributed Security*, *supra* note 3*; see also* Robinson & Darley, *The Utility of Desert*, *supra*, 91 Nw. U. L. Rev. at 476.

[134]Homicide laws ("do not take another person's life") and theft laws ("do not take another person's property") are examples of "do not" laws. *See, e.g.*, MODEL PENAL CODE §§ 210.1, 223.2.

[135]*See supra* notes 124 - 133 and accompanying text

[136]*See supra* Part II(A)(4). Seat-belt laws are not concerned with preventing crime; they are generally regarded as public health and safety measures. *See, e.g.,* Ilise Levy Feitshans, *Foreshadowing Future Changes: Implications Of The Aids Pandemic For International Law And Policy Of Public Health*, 15 MICH. J. INT'L LAW 807, 810 (1994).

no crime was committed. We would in effect be holding someone criminally liable for failing to prevent something that did not happen.[137]

The fact that using "do" laws to achieve citizen participation in combating cybercrime is inconsistent with how we approach criminal liability is important, not because it goes against the way we do things, but because we must use legal principles to create new behavior patterns. If the principles we use are inconsistent with embedded expectations and understandings, they will be met with resistance and will not create the desired behavior patterns.[138] We need an approach that does less violence to societal expectations. Parts II(B) and II(C) outline such an approach.

B. CYBERRULES

On the Internet, nobody knows you're a dog.[139]

The discussion in Part II(A) speaks of establishing "citizen" responsibility for preventing cybercrime and, in so doing, suggests we would impose a single, monolithic requirement upon all citizens to "prevent cybercrime." This is neither feasible nor reasonable. Instead, we should change attitudes and assumptions so that "citizens," i.e., those who are not by profession charged with preventing and reacting to criminal activity, come to play an active role in securing cyberspace. However, relying on simplistic, draconian rules that require everyone to "prevent cybercrime or face the consequences" would be futile and counterproductive.

Thus, what we need is a new set of rules for making certain assumptions a part of the store of knowledge people use in their everyday life. We want people's responsibility for

[137]We do impose criminal liability for crimes that are not consummated, but only when some steps have been taken toward the commission of an offense. *See, e.g.,* Model Penal Code §§ 5.01-5.03 (attempt, conspiracy and solicitation).

[138]*See, e.g.,* MARTIN ALAN GREENBERG, AUXILIARY POLICE: THE CITIZEN'S APPROACH TO PUBLIC SAFETY 14 (1984)*; see also supra* note 133.

[139]Peter Steiner, Cartoon, 69 The New Yorker 61 (July 5, 1993), http://www.epatric.com/funstuff/dog/.

preventing cybercrime to become an embedded assumption that is inherent in their daily lives in the same way that, for instance, using smoke detectors or not speeding in school zones is part of the general fabric of everyday life. Not everyone will strive to prevent cybercrime with the requisite diligence, but some percentage of those whose conduct falls below the required standard of care will be identified and sanctioned for their failures. If the rules we implement are sufficiently discriminating and if the sanctions we impose are appropriately calibrated to reflect an offender's culpability, this adventitious system of enforcement should suffice to ensure an adequate level of compliance, just as it does in other areas of criminal law.

In fashioning this differentiated set of rules, we must begin with a fundamental dichotomy that allocates citizens into two categories and derives from the posture individuals and entities assume as to cyberspace.[140] Most citizens participate in cyberspace for professional or personal reasons but play no role in constructing it; they are "users" of cyberspace. The other category consists of individuals and entities that do play roles in constructing cyberspace. They design, create or supply the software and hardware that is employed to create and sustain the collective experiential phenomenon we know as cyberspace;[141] they are the "architects" of cyberspace.

This dichotomy is essential because the posture one assumes as to cyberspace determines the type of preventative measures it is reasonable to require of that person or entity. The difference between "users" and "architects" is one of control. "Users," whether individuals or

---

[140]*See, e.g.,* Tania Brief & Terrell McSweeny, *Corporate Criminal Liability*, 40 AM. CRIM. L. REV. 337, 337-47 (2003); United States v. Park, 421 U.S. 658, 667-73 (1975).

[141]*See, e.g.,* Gordon Fletcher, . . . *Towards an Anthropology of Cyberspace,* Spaceless.com (1997), http://www.spaceless.com/papers/14.htm ("The tools that construct the Internet — the software, the hardware, the protocols and the network — which are all material culture items themselves produce . . . cyberspace"). *See also* Anita Greenhill & Gordon Fletcher, . . . *The Social Construction of Electronic Space,* Spaceless.com (1997), http://www.spaceless.com/papers/12.htm. For cyberspace as an experiential phenomenon, *see infra* notes 156-159.

entities, can control only their own conduct.[142] Their efforts are essentially defensive; "users" must defend themselves against those who would victimize them. As such, "users" are on the front lines of the battle between order and cyberdisorder. They must use their best efforts to employ the tools (i.e., hardware, software) made available to them so as to secure their systems from attack and otherwise fend off the attentions of cybercriminals. The rules that target "users" would therefore emphasize one's responsibility not to become a victim and the consequences attendant upon defaulting on that obligation.

Although not all "users" are "architects", all "architects" are "users" at some time. When "architects" are simply participating in cyberspace, they are "users" and will therefore be subject to the "user" rules outlined in Part II(C)(1). Yet, it is necessary and reasonable to impose additional obligations upon "architects" when they are acting in their respective capacities as "architects," i.e., as the devisers and purveyors of the implements "users" employ to participate in cyberspace and protect themselves while doing so. Imposing these additional obligations upon "architects" is necessary because "architects" determine the potential for security in cyberspace; it is reasonable to impose such obligations upon them because they can exercise more control over security in cyberspace than can "users."

Cyberspace is often analogized to the American Wild West, but that is an imperfect analogy. As a social and cultural event, the American West was the process of expanding nineteenth-century American institutions and culture into the "unsettled" areas of the country; guarantees of internal order were concededly intermittent and fragmented in these areas until the process was complete. But this did not lead to the *absence* of order; rather, the lapses and gaps in internal order that characterized this process were irregularities and were recognized as such.

[142]As Part II(B)(1) explains, "users" can also be required to exercise some supervision over the conduct of others, e.g., parents can be required to supervise the conduct of their children.

Internal order prevailed in the eastern half of the country and everyone realized it would eventually prevail in the West as well. [143]

Cyberspace is more appropriately compared to Europe during the Dark Ages, i.e., the six to eight centuries following the fall of Rome.[144] "The decline of Rome, the collapse of structure, of law and order . . . left western Europe bereft of political cohesion" and ravaged by natural forces.[145] Like cyberspace, Europe during these disordered times was a "place" where presumptive order simply did not exist.[146] Theft, rape, murder and other crimes were rampant,[147] but "given the general indifference of medieval populations to crime in areas other than their own, apprehension . . . was very unlikely."[148] Criminals used the primarily rural terrain to avoid apprehension; robbers, burglars, kidnappers and "assassins . . . slipped back into the anonymous countryside once their deeds were done."[149] The reign of misrule was exacerbated by law-abiding citizens who had no qualms about using crime as an "intermittent supplement" to their regular sources of income.[150] The presence of outlaws made commerce difficult; travelers carried weapons and banded together, "seeking collective security."[151]

---

[143]*See, e.g.,* Dan Gillmor, *In the Wild West of the Internet, There are Good Guys and Bad Guys,* SiliconValley.com (September 28, 2003), http://www.siliconvalley.com/mld/siliconvalley/6881523.htm.

[144]*See, e.g.,* WILLIAM MANCHESTER, A WORLD LIT ONLY BY FIRE: THE MEDIEVAL MIND AND THE RENAISSANCE 3-5 (1992).

[145]TERRY L. GORE, NEGLECTED HEROES: LEADERSHIP AND WAR IN THE EARLY MEDIEVAL PERIOD 3 (1995)*; see also* MANCHESTER, *supra* note 144, at 5.

[146]*See, e.g.,* CAROLLY ERICKSON, THE MEDIEVAL VISION: ESSAYS IN HISTORY AND PERCEPTION 148-80 (1976).

[147]Burglary, counterfeiting and other currency offenses were also common. *See id.* at 164-66, 171.

[148]*Id.* at 163. "Because of this, the majority of medieval lawbreakers never came into contact with the law . . . at all." *Id.*

[149]*Id.* at 155. As late as 1500, eighty to ninety percent of the population "lived in villages of fewer than a hundred people, fifteen or twenty miles apart, surrounded by endless woodlands." MANCHESTER, *supra* note 144, at 50-51.

[150]ERICKSON, *supra* note 146, at 163.

[151]Manchester, A World Lit only by Fire, *supra* at 64-65

How does comparing cyberspace and early medieval Europe advance our effort to devise rules that will encourage citizens to assume responsibility for preventing cybercrime? The comparison is instructive because it demonstrates the similarities – and dissimilarities – of the two. Like early medieval Europe, cyberspace is a "place" where order is problematic because the devices traditionally used to create and sustain order are ineffective.[152] Yet, the two differ as to the reasons why order is problematic. Disorder was ultimately a transient phenomenon for medieval Europe; it was the product of a number of factors, including Rome's

[152]Real-world systems must establish and maintain internal and external order if they are to survive. *See supra* § I. This principle cannot be extrapolated to cyberspace because it is not a "place." *See* infra notes 156-159 and accompanying text. Since cyberspace is not a "place" with fixed, identifiable boundaries separating it from other "places," the distinction between internal and external order has no meaning. One could argue that there is a relevant boundary: the boundary between the real-world and cyberspace. If we were to accept this argument, our focus would be on maintaining order "in" cyberspace and order "between" cyberspace and the real-world. The problem is that this argument assumes cyberspace is a "real" place when it is not. There is no cyberspace without the real-world; cyberspace exists only insofar as we humans, creatures of the real-world, engage in the activities and employ the technologies that create and sustain the collective experience we know as cyberspace. *See* infra notes 156-159 and accompanying text. The "border" between the real-world and cyberspace is experiential, not geographic; the more precise focus is therefore upon establishing order in the intricate myriad of communicative processes we experience as cyberspace.

Until Rome fell, Europe relied on its institutions establish and maintain internal order; after Rome fell, those institutions no longer existed and the rules they implemented were no longer effective. *See, e.g.,* Norman F. Cantor, THE CIVILIZATION OF THE MIDDLE AGES 40-47 (1993); Manchester, A World Lit only by Fire, *supra* at 3-5. The disorganizing effect of Rome's fall was exacerbated by invasions of tribes which had their own rules and institutions. *See, e.g.*, Paul Vinogradoff, *Foundations of Society (Origins of Feudalism),* 2 Cambridge Medieval History 630 (1913), http://msnbc.msn.com/id/3078827/. ("influx of . . .barbarians was bound to break up the frame of Roman civilization" but what made matters worse was that they "had come with social arrangements of their own"). A level of internal order naturally existed in Europe even during the Dark Ages; had it been totally lacking, the population would have died out or emigrated in search of more stable environments. *See supra* note 5 and accompanying text. But Europe during the Dark Ages is still the best real-world analogy for cyberspace because it is a period when basic institutions and basic social life were in disarray; such widespread, formless disarray was never typical of the American West, as it always had an anchor in the "civilized" society east of the Mississippi.

collapse and the ensuing vacuum into which poured an unstable mix of cultures and alliances.[153] The demise of disorder and the re-imposition of order in Europe were inevitable because real-world systems *require* internal and external order if they and their constituent populations are to survive and endure.[154] When a real-world system descends into anarchy, the loss of internal order is necessarily a temporary state; the entities populating the system must re-establish order, migrate to other social systems, or cease to exist, both individually and collectively.[155]

The same is not true of cyberspace. Order is not inevitable in cyberspace because it is not a "place"; it is instead, as William Gibson said in *Neuromancer*, a "consensual hallucination".[156] Physical analogies are inapposite because cyberspace is not a locus, it is an activity -- a complex type of mediated communication.[157] We do not "inhabit" cyberspace, nor do we "visit" cyberspace; we "do" cyberspace, i.e., we experience an intricate, multi-layered communicative process that is sustained by a series of increasingly complicated technologies.[158] A decade or so ago, we fell into the habit of referring to this experience as a "place" because we

---

[153]*See also* CANTOR, *supra* note 152, at 89-121.

[154]*See supra* Part I. For the establishment of order in medieval Europe, *see, e.g.,* CANTOR, *supra* note 152, at 483-528.

[155]*See* Brenner, *Distributed Security*, *supra* note 3*; see also supra* note 5 and accompanying text.

[156]WILLIAM GIBSON, NEUROMANCER 51 (1984).

[157]*See, e.g.,* Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution,* 7 J. TECH. L. & POL'Y 124, 131 (2002), http://grove.ufl.edu/~techlaw/vol7/2/brenner.pdf:

> Mediated communication is communication that takes place via some artificial medium (such as the telephone); it is distinguishable from direct, or face-to-face, communication. Mediated communication can be specifically directed at one or more known parties . . . or it can be disseminated generally to an unidentified audience, such as in radio or television broadcasts. Mediated communication can also be interactive . . . or it can be the unilateral transmission of information, such as with radio or television broadcasts.

For more on mediated communication and cyberspace, *see id.* at 131-133.

[158]*See id.*

are creatures of the real-world and, as such, we have no conceptual referent that accurately encompasses this process to which many of us devote a great deal of our time.[159]

We did not confront this issue with earlier types of mediated communication. Written correspondence is not real-time and therefore posed no conceptual difficulties; corresponding (i.e. writing) and perusing correspondence (i.e. reading) fell into known, established categories of experience.[160] Telephonic communication required more of an adjustment because although it is real-time, it is not face-to-face discourse; nonetheless, as real-time communication, humans

---

[159]John Perry Barlow claims he first applied Gibson's "science fiction term Cyberspace to the . . . global electronic social space now . . . referred to by that name. Until his naming it, it had not been considered any sort of place." Barlow@eff.org. John Perry Barlow, *Barlow Home(stead) Page*, *at* http://www.eff.org/~barlow/barlow.html (last visited Sep. 26, 2004). *See supra* note 156*; see also* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, http://www.eff.org/~barlow/Declaration-Final.html (last modified Feb. 8, 1996).

A "conceptual referent" is a framework we use to "make sense of" experience. A concept is a schema for evaluating objects and events that "serves as a psychological yardstick" for comparing and evaluating stimuli. O.J. Harvey, David E. Hunt & Harold M. Schroder, Conceptual Systems and Personality Organization 10-11 (1961). Objects and experiences "have no psychological value" until they are "compared to a conceptual referent." *Id.* at 13. New technologies require us to develop conceptual referents so we can fit new experiences into our understanding of the world. *See infra* notes 157- 158 and accompanying text. For lack of a better model, we have chosen to conceptualize the complex process of computer-mediated communication that has proliferated over the last decade or so as a "place," a variation of the real-world. *See, e.g.*, Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, *supra* note 157, at 160:

> Because of the way cyberspace is . . . configured, it is . . . almost irresistible, to think of it as a virtual place, a contrived mirror of the real world. . . .[M]uch of what we experience in the real world — streets, buildings, . . . vehicles . . . etc. — is also contrived, the product of human intelligence and effort. In the real world, these contrivances must . . . operate within certain . . . constraints. Pool tables . . . must have legs . . . In the virtual world . . . these constraints no longer hold true. Pool tables . . . do not require legs in this place where gravity does not exist. Logically, . . . there is no reason why that place should resemble the real world. The only reason why cyberspace . . . mirrors the . . . real world is because those who originally settled . . . cyberspace . . . assumed that this virtual place should operate according to the same constraints that prevail in the real world.

[160]*See id.* at 131-133.

quickly adapted to the phenomenon of being "on the phone," i.e., of speaking with one whose physical location is more or less remote.[161] The complex, computer-mediated communicative process we call "cyberspace" is a much more substantial challenge. Some aspects of this process are analogous to an exchange of written correspondence that takes place in real-time or almost-real-time, except that we may have no idea as to the identity, location or other bona fides of the person with whom we are corresponding. Other aspects are analogous to "publishing" or "broadcasting" content (words, graphics, music, etc.) in the real-world. This intricate network of computer-mediated communication frees us from the commercial constraints of publishing houses and movie studios and lets us, for better or worse, share our ideas and creativity with the world. Increasingly, however, aspects of this process bear no relationship whatsoever to the objects and events we are familiar with from the real-world.[162] In cyberspace, for instance, I can experience virtual worlds, participate in multi-player online games of varying degrees of violence and unreality, or create an alternate life in a virtual community.[163] I can

[161]*See id.* Other types of mediated communication, including the telegraph, radio, cinema and television, required some adjustment but none presented the conceptual challenges posed by cyberspace. The telegraph, which was never available for private use and therefore had a limited effect upon the public, was conceptually analogous to the telephone; that is, it involved real-time distance communication with one other person. *See id.* Radio, cinema and television differ from written, telephonic and telegraphic communication in that they all involve passive communication; that is, content generated by one (or several) is disseminated to individuals who merely "receive" it. *See id; see also supra* note 157. The delivery mechanism used in these technologies was novel, but the communicative process was not. Radio, television and the cinema are functionally analogous to the plays, operas, vaudeville shows and other "live" performances humans have enjoyed for millennia; we were accustomed to being part of an "audience" and that gave us the conceptual reference we needed to adapt to these technologies.

[162]The capacity for un-real-world experience increases as the sophistication of the technologies used in the process increases; the early Internet was primarily text-based and therefore offered little in the way of "virtual" experiences. *See, e.g.*, James W. Dow, *The Early History of Electronic Communication in Applied Anthropology*, American Anthropological Association (1999), http://www.aaanet.org/napa/ publications/napa19/three/threea.html.

[163]*See, e.g.*, Ultima Online, http://www.uo.com/; Battle.net, http://www.battle.net/intro.shtml; Real Sims Online, http://www.realsimsonline.com/index.asp; Theatre des Vampire, http://www.visi.com/~rioghnach/ gothicquarter/.

enjoy experiences that are distinctly unreal,[164] I can commit crimes, and I can combine the two.[165] To comprehend these varied experiences and incorporate them into my understanding of reality, I need to have an empirical phenomenon to act as a source of analogy, or as a conceptual referent, for them.[166] We could have developed discrete referents, using different empirical analogies for various aspects of this process; however, we have instead chosen to use the concept of "place" as our comprehensive referent, perhaps because it seems the experiences we have online must "take place" in some unknown "space." [167]

There is nothing objectionable about using "space" as the conceptual referent for online experience as long as we do not come to believe that this "space" is real. Our experiences creating and maintaining order in human social systems have so far been limited to the real-world, where order is difficult to escape. In the real-world, conduct, which is at once the source of order and disorder, is embodied and situated in physical space; because it is subject to the physical constraints of the real-world, conduct is visible, traceable and controllable with the use of social and physical force.[168] Except for occasional exceptions (e.g. hermits, castaways), humans live in societies because they need the physical and emotional support other humans provide.[169] Most conduct is therefore "visible" to those with whom one shares a social system; since it is visible, conduct can be traced to the actor, who can be held accountable for what she

[164]*See, e.g.*, Julian Dibbell, *I Feel Pretty*, *in* MY TINY LIFE (1998) (describing his experience with "virtual womanhood" in a virtual community), http://www.juliandibbell.com/mytinylife/tinyexcerpts_pretty.html.

[165]*See, e.g.*, Julian Dibbell, *A Rape in Cyberspace*, *in* MY TINY LIFE (1998) (describing multiple-victim rape in a virtual community), http://www.juliandibbell.com/texts/bungle.html.

[166]*See supra* note 159.

[167]*See, e.g.*, Barlow, *A Declaration of the Independence of Cyberspace*, *supra* note 156 ("Cyberspace consists of transactions, relationships, and thought . . . arrayed . . . in the web of our communications").

[168]*See supra* Part II(A)(1)-(2).

[169]*See, e.g.*, F.L.K. HSU, CLAN, CASTE AND CLUB 149-158 (1963); TALCOTT PARSONS, THE SOCIAL SYSTEM 251-256 (1951); GEORGE C. HOMANS, THE HUMAN GROUP 128-192 (1950).

did or failed to do.[170] Humans are held accountable either formally or informally.[171] Most of the control exercised in human societies is informal.[172] Individuals learn that certain behaviors are "right" or "appropriate;" they also learn that they will receive approval and rewards if they behave in the "right" or "appropriate" ways, but will suffer disapproval if they behave in ways that are "wrong" or "inappropriate."[173] This is an effective way of maintaining internal order because people "obey the rules not because they are forced to, but because they want to."[174] While this is an effective way of maintaining internal order, it is not perfect. Since not everyone obeys the rules, societies use formal social control against those who violate their more important rules, i.e., their proscriptive rules.[175] Criminal justice systems impose various types of sanctions on those who violate proscriptive rules on the assumptions that (i) sanctions will deter the person from re-offending and (ii) sanctioning her will deter others from

---

[170]*See id.*

[171]ALAN S. MILLER & SATOSHI KANAZAWA, ORDER BY ACCIDENT: THE ORIGINS AND CONSEQUENCES OF CONFORMITY IN CONTEMPORARY JAPAN 8-9 (2000):

> [A]n important distinction is between informal and formal . . . social control . . . . Informal social control has a wide variety of components that run from basic socialization . . . to peer pressure and informal group monitoring and sanctioning. The focus is on ways that normative . . . behavior is taught and reinforced . . . . Formal social control refers . . . to the criminal justice system, and . . . enforcing social norms that are seen as important enough to have been codified into laws.

[172]*See id.* at 9 (the overwhelming percentage of people follow rules "because of informal social control . . . .[P]eople have been socialized to follow society's rules, and they interact in social situations where behavioral conformity is rewarded"). *See also supra* notes 109-112.

[173]*See* MILLER & KANAZAWA, *supra* note 171, at 9 ("through informal group monitoring, inappropriate behavior is quickly detected and punished"). *See also supra* notes 168-169.

[174]MILLER & KANAZAWA, *supra* note 171, at 9.

[175]*See id.* at 9, 67*; see also supra* notes 21-23 and accompanying text.

offending.[176] In the real-world, internal order, despite being imperfect, is ubiquitous; it is appropriately our default assumption.

That is the real-world, where conduct is embodied and situated in physical space. In cyberspace, the same is not true. This difference is important for our analysis of how order can be maintained "in" cyberspace. Having a defined, delimited population that is situated in physical space which is controlled and secured from external threats has been the basis of internal order since human societies began.[177] Order is ubiquitous because it is inescapable. Members of a society learn to obey the rules that sustain internal order; yet, while internalizing the rules offers some assurance that individuals will obey them, it is not enough. The obligation to obey the rules must be reinforced. This reinforcement comes from interacting with others whose approval we desire, and whose disapproval we fear, in a spatial context where our behavior can easily be observed and assessed.[178] This reinforcement process is integral to the social control systems outlined above.[179] Although it is the *raison d'etre* of the informal system, it is also important for the formal system. When subject to a formal system, we know that our actions in the real-world can be observed, and therefore we realize that there is some risk of being caught if we violate a proscriptive rule.[180] Our awareness of that risk and our desire to

---

[176]*See, e.g.,*JACK P. GIBBS, A THEORY ABOUT CONTROL 255-257 (1994)*; see also supra* notes 21-23 and accompanying text.

[177]It is also the basis for maintaining order in other systems. *See* Brenner, *Distributed Security*, *supra* note 3, at 2-3.

[178]*See, e.g.,* Richard A. Posner & Eric B. Rasmussen, *Creating and Enforcing Norms,with Special Reference to Sanctions,* 19 INT'L REV. L. & ECON. 369, 372-77 (1999); Harold G. Grasmick & Donald E. Green, Legal Punishment, *Social Disapproval and Internalization as Inhibitors of Illegal Behavior*, 71 J. CRIM. L. & CRIMINOLOGY 325, 334 (1980).

[179]*See supra* notes 169-176 and accompanying text.

[180]Research shows that the deterrent effects of sanctioning those who commit crimes "are more strongly associated with people's estimates of the likelihood of being . . . than they are by the anticipated severity of punishment. *See* Tom R. Tyler, *Procedural Justice, Legitimacy and the Effective Rule of Law*, 30 Crime & Just. 283, 303 (2003).

avoid the consequences attendant upon being caught violating such a rule are credible disincentives for doing so.[181]

While this process is a compelling force in small communities, it is also an essential element of modern, urbanized society.[182] Its importance is most evident when the bounds of the spatially-based real-world system of order begin to fray and people behave in ways other than those dictated by their internalized rules. A good example of this is behavior in motor vehicles. "Most of us have . . . observed that driving an automobile can alter a person's behaviour from civility to incivility; in some cases, otherwise normal people become violent when they are behind the wheel of a car."[183] One explanation for this is that our visibility, or our perception of

[181]*See, e.g.*, Harold G. Grasmick & Robert J. Bursik, Jr., *Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model*, 24 LAW & SOC'Y REV. 837, 841 (1990) (suggesting three kinds of potential costs considered by individuals in deciding whether to obey the law). Conversely, if we think there is little chance we will be observed and "caught", we are more likely to violate rules, even proscriptive rules, especially if the penalties are small*; see, e.g.*, Margaret Raymond, *Penumbral Crimes*, 39 AM. CRIM. L. REV. 1395, 1404 (2002) (stating that drivers speed because they believe "they will not be subjected to social disapproval for speeding" and "will suffer no sanction for it").

[182]*See supra* notes 178 and 181.

[183]M. E. Kabay, *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy*, Address Before Annual Conference of the European Institute for Computer Anti-virus Research 8 (Mar. 1998), http://www2.norwich.edu/mkabay/overviews/anonpseudo.pdf, (last visited September 28, 2004)*; see, e.g.*, Kent Walker, *The Costs of Privacy*, 25 Harv. J.L. & Pub. Pol'y 87, 101 (2001):

> Anonymity can . . . operate as the cloak of night – promoting negative behavior and disregard for the rules that organize social interaction. Imagine a society of complete anonymity**.** We already have a pretty good proxy: the freeway -- the arena of rudeness, abuse, discourtesy, road rage . . . . It is hard to imagine people acting in the grocery store the same way that they behave on the freeway – pushing their carts ahead of others in line and making nasty gestures to people in the aisles. The incentives for good behavior grow stronger when you are in your neighborhood, your office, or your local store – anywhere you know the other shoppers and they know you.

our visibility, is reduced when we operate a vehicle; that perception of reduced visibility, of anonymity, erodes our sense of social responsibility.[184]

The same is true – but to an even greater extent -- of our participation in cyberspace. While we can attain a level of anonymity in the real-world, in the cyber-world we can achieve complete anonymity and thereby divest ourselves of the embodied, physically situated life of the real-world and the behavioral constraints it imposes.[185] This certainly does not mean that

---

[184]*See* Kabay, *supra* note 183, at 6-7 (explaining the meaning of identity and summarizing the importance of personal identification); *see, e.g.,* Walker, *supra* note 183 and accompanying text; *see also* Deborah Lupton, *Road Rage: Drivers' Understandings and Experiences*, 38 J. OF SOCIOLOGY 275, 280 (2002) ("[D]riving is like a sense of freedom….I can feel the car….I can control it, I can go wherever I want….I can do whatever speeds I want. I can break the law if I want….") (interviewing a university student). According to social psychologists, perceived anonymity erodes the influence of internalized norms and contributes to deindividuation and antisocial behavior; *see* Kabay, *supra* note 183, at 8 (noting that deindividuated people display reduced inhibitions and "reduced reliance on internal standards that normally qualify their behaviour"); *see, e.g.,* Dwight A Hennessy & David L. Wiesenthal, *Gender, Driver Aggression, and Driver Violence: An Applied Evaluation*, SEX ROLES: A JOURNAL OF RESEARCH 7 (June 2001), http://www.findarticles.com/cf_dls/m2294/2001_June/80805131/p1/article.jhtml, (last visited September 29, 2004) ("[T]he anonymity of the driving environment and perceptions of deindividuation represent a unique opportunity for liberation . . . thus facilitating the expression of aggressive tendencies. . . . [T]he potential for personal repercussions as a result of aggressive behaviors are minimized with anonymity, leading to a heightened sense of control . . . ."); *see also* Cashton B. Spivey & Steven Prentice-Dunn, *Assessing the Directionality of Deindividuation: Effects of Deindividuation, Modeling, and Private Self-Consciousness on Aggressive and Prosocial Responses*, 11 BASIC AND APPLIED SOCIAL PSYCHOLOGY 387, 398-99 (1990) (explaining that subjective deindividuation renders individuals susceptible to environmental influences).

[185]*See, e.g.,* Kabay, *supra* note 183, at 13:

> [A]nonymity and pseudonymity are possible using older means of communication: people have thrown rocks through windows, sent anonymous vituperation through the mail, and harassed people with anonymous phone calls for millennia, centuries and decades respectively. Such behaviour has historically been of relatively minor importance. How is it that anonymity and pseudonymity seem so important in cyberspace? . . . One factor is the ease with which one *can* be untraceably anonymous in cyberspace. . . .

See also supra note 63 and accompanying text. The partial anonymity we enjoy while operating a motor vehicle loosens the social restrictions we otherwise operate under but only for a limited period of time and only for limited purposes; however, when we go online, we can be completely anonymous (or pseudonymous) for as long as we like,

everyone who ventures into cyberspace cloaks themselves in anonymity and embarks upon a career of antisocial or even illegal acts. In fact, much of what have seen so far, in terms of online behavior, has been the transposition of real-world patterns of civility onto the Internet.[186] It is, however, clear that people are taking advantage of the liberation they feel online to engage in behaviors they would never have felt free to indulge in the real-world.[187] One most dramatic example of this involves child pornography; cyberspace has "caused explosive growth in the market for child pornography."[188] Much of this growth is due to individuals who would never

---

we can repeat the experience whenever we choose, and we can put our anonymity to various uses. *See, e.g.*, Brenner, *supra* note 157, at 138-40. The facility with which one can become anonymous or pseudonymous in cyberspace has given rise to the concept of "nymity", i.e., the extent to which an online persona is fictitious. *See, e.g.*, Nymity, *at* http://www.nymity.com/about_us/, (last visited September 29, 2004) (defining the word "nymity" as "the degree of anonymity")*; see also Lance Detweiler & The Theory of Nymity*, GEEK TIMES (2004), *at* http://www.geektimes.com/michael/culture/humor/items/Geekish/theoryOfNymity.html, (last updated September 8, 2004).

[186]*See, e.g.*, Andrew P. Morriss, *The Wild West Meets Cyberspace*, THE FREEMAN: IDEAS ON LIBERTY (July 1998), at 2, *available at* http://www.fee.org/vnews.php?nid=4074, (last visited September 29, 2004) ("[M]illions of users have managed to adopt standardized protocols enabling the network to function, social norms have arisen in a wide range of contexts, norms that are enforced by communities of users. . . . ").

[187]*See, e.g.*, Gaylen Duncan, *CyberCrime*, Address Before the International Information Industry Congress 2000 Millennium Congress 3 (September 19, 2000), *available at* http://www.itac.ca/Library/PolicyandAdvocacy/CyberSecurityandPrivacy/pdf/00Oct23-crime-iiic.pdf, (last visited September 29, 2004) ("The level of anonymity conferred by the Internet, combined with the lack of perceived consequences for inappropriate behaviour in cyberspace, means that standards of conduct displayed on the Internet often fall short of those exhibited offline.").

[188]*Enhancing Child Protection Laws After the April 16, 2002 Supreme Court Decision, Ashcroft v. Free Speech Coalition: Hearing Before the Subcommittee on Crime, Terrorism and Homeland Security of the House Committee on the Judiciary*, 107th Cong. 8 (2002) (statement of Michael J. Heimbach, Unit Chief, Crimes Against Children Unit, Federal Bureau of Investigation), *available at* http://www.house.gov/judiciary/79366.PDF, (last visited September 29, 2004)*; see also* John Carr, *Child Abuse, Child Pornography, and the Internet: Executive Summary* 1 (2004), http://www.nch.org.uk/downloads/children_internet_report_summ.pdf, (last visited September 29, 2004) (stating that the internet has created new ways for pedophiles to reach and abuse children, as well as creating new ways to distribute images of such sexual abuse). For example, in 2001, Thomas Reedy was imprisoned for

have sought out child pornography in the real-world, where obtaining such material would be difficult and dangerous; on the Internet, however, they can obtain it easily and with relatively little risk.[189] As this is true of child pornography, it is also true, in varying degrees, of other types of illegal conduct.[190]

Although the focus of this discussion is not on those who commit crimes, the capacity of cyberspace to create a climate in which the bonds of social conformity are eased, if not eradicated, is relevant to the issues under consideration. It establishes the need to recruit citizens into the process of online law enforcement; as the discussion above demonstrates, the experiential "world" of cyberspace erodes the forces which maintain order in the real-world and defeats law enforcement efforts to apprehend those who violate the rules that prevent citizens

---

operating an "online child porn empire" that stretched "across three continents, some 250,000 subscribers and a turnover of $1.4m a month." *Operation Avalanche: Tracking Child Porn*, BBC NEWS (November 11, 2002), at 1, *available at* http://news.bbc.co.uk/1/hi/uk/2445065.stm, (last visited September 24, 2004). *See also* Carr, *supra* at 1 ("In 2003 one man in Lincolnshire was found with 450,000 child abuse images and a private individual in New York was found with 1,000,000.").

[189]*See, e.g.*, Heather Maher, *Online and Out of Line: Why is Cybercrime on the Rise, and Who's Responsible?*, ABC NEWS (January 20, 2000), *at* http://more.abcnews.go.com/sections/us/DailyNews/cybercrime_000117.html, (last visited ___):

> The cloak of anonymity brings these people to the surface. . . . If these individuals, precomputer, had wanted to engage in this type of behavior, they'd have to leave their homes and interact with someone. [The Internet] is two levels removed from that—they are in the comfort of their home, or cubicle at work, they are in their own environment, which lessens the stress. You can pick whatever chat room name or e-mail you want, and…that allows people to go where they wouldn't go before.

Those who acquire and trade child pornography online use pseudonyms and encryption to conceal their identities and avoid apprehension*; see, e.g.*, William R. Graham, Jr., Comment, *Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to 'Wonderland'*, 2000 L. REV. M.S.U.-D.C.L. 457, 465. The ease with which child pornography can be obtained online not only increases the number of those who acquire and possess child pornography, it has led to an increase in the size of the rings that create and distribute child pornography*; see, e.g.*, Graham, *supra* at 461-65.

[190]*See, e.g.*, World Federation of Scientists, *supra* note 4, at 7-9.

from preying upon each other. The reactive, offensive mode of law enforcement is ineffective in this context. We must instead adopt a defensive model in which citizens assume responsibility for preventing their victimization and the victimization of those for whom they are held accountable.[191] While citizens cannot prevent all cybercrime, placing the burden upon them to prevent their own victimization will reduce the opportunities available to those who wish to commit crimes and thereby improve our ability to maintain order in the experiential environment of cyberspace. Also, requiring citizens to take reasonable efforts to prevent cybercrime may overcome cyberspace's erosive effects and reinforce the influence of the norms and laws that maintain internal order in the real-world. At the very least, it emphasizes our intention to maintain a baseline of order in this experiential world comparable to that which prevails in the real-world.

C. "USERS" AND "ARCHITECTS"

Since "users" of cyberspace only control their own conduct,[192] all we can ask of them is a reasonable effort to prevent cybercrime using the tools available to them; the rules outlined in Part II(C)(1) below define this expectation. Such a collective effort will, without more, enhance the overall security of cyberspace, but it will be more effective if the "architects" of cyberspace apply their talents to the effort as well. Since "architects" create and supply the tools "users"

[191] *See, e.g.*, Joris Evers, *European Commission to Set Up Pan-European Cybercrime Forum*, INFOWORLD (December 5, 2000), at 2, http://archive.infoworld.com/articles/hn/xml/00/12/05/001205hncyberforum.xml, (last visited September 29, 2004) ("'We can't give all responsibility to the police, you [the Internet user] are also responsible for keeping a safe virtual environment on the "Net" [sic]) (quoting Antonio Vitorino, European Commission Justice and Home Affairs Commissioner).

[192] *See supra* Part II(B).

rely upon,[193] they are in a position to enhance the efficacy of those tools. Part II(C)(2) considers methods by which "architects" can be recruited into this effort to prevent cybercrime.

1. "Users"

> *Each American who depends on cyberspace . . . must secure the part . . . for which they are responsible.*[194]

The purpose of the "user" rules is to undo assumptions derived from the triumph of the professional, reactive model of law enforcement in the real-world.[195] The goal is to require citizens to assume responsibility for protecting themselves from cybercrime and cybercriminals; the result, to some extent, is a return to an older, distributed model of law enforcement.[196]

The first rule imports assumption of risk into criminal law. Assumption of risk emphasizes the need to protect oneself from the risks in cyberspace; thus, its purpose is to negate citizens' expectations that their victimization will produce an effective law enforcement reaction. The second rule uses complicity to impose liability for conduct that contributes to the commission of a cybercrime against another; it proscribes not the *failure to prevent* cybercrime, as such, but the act of *contributing to the commission* of a cybercrime.

(a) Assumption of Risk[197]

Assumption of risk may seem a peculiar choice for this endeavor since, in tort law, the principle of assumed risk negates liability instead of imposing it.[198] In fact, assumption of risk,

---

[193]*See supra* Part II(B).

[194]*See, e.g.,* Office of the President, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 11 (February 2003), http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf, (last visited September 29, 2004).

[195]*See supra* Part I.

[196]*See supra* Part I.

[197]*See* Brenner, *Toward a Criminal Law for Cyberspace: A New Model for Law Enforcement?*, *supra* note 3, at 71-104, for a more detailed treatment of this alternative.

or more appropriately a modified conception of assumed risk, could markedly advance this effort.

In tort, if one is found to have assumed the risk of the danger that caused her injury, she is barred from obtaining redress for that injury.[199] We cannot import this particular doctrine into the criminal law governing cyberspace, since doing so would deny the possibility of justice to those who could be deemed to have assumed the risk of their victimization. Criminals would, in effect, be given a "get-out-of-jail-free card" for victims who did not and/or who could not protect themselves. Such a result is clearly unacceptable. We want citizens to prevent cybercrime to the extent they can reasonably be expected to do so; but we certainly do not want to declare open season on the civilian populace of modern societies by declaring that no prosecutions can be brought if the victim did not take acceptable precautions to prevent being victimized. We need to impose a level of assumed risk and yet still retain the capacity to prosecute even when a victim's precautionary efforts were less than adequate.

We could do this with a modified assumption-of-risk principle containing two elements: (i) a proposition negating the expectation of a law enforcement reaction to victimization; and (ii) a statement that the negation of such an expectation does not bar the investigation and prosecution of cybercriminals. The principle might look something like this:

(1) One who [understanding the risk of harm to self or property] accesses or employs cyberspace to engage in activity without having taken all reasonable measures to protect herself and her property from being victimized by criminals during the course of and with regard to any matters related to that activity shall be deemed to have assumed the risk of victimization resulting from that activity. One who has been victimized should report the

[198] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS §§ 496B-496C (1965).

[199] *See id.*

offense(s) to the appropriate law enforcement agency. The filing of such a report in no way obligates the agency to investigate or to otherwise pursue the matter; domestic law enforcement agencies have full discretion to determine what, if any, action will be taken as the result of their receiving such a report. Law enforcement agencies are under no obligation to take action with regard to offenses targeting those who assumed the risk of becoming a victim online, though they may do so.

(2) The fact that one assumed the risk of being victimized pursuant to paragraph (1) creates no enforceable rights in person(s) who contributed to that victimization. The principles set forth in paragraph (1) cannot be used as an affirmative defense in a prosecution for offenses committed against one who assumed the risk of being so victimized or in a civil action brought for injuries or damages resulting from the commission of such an offense; these principles in no way restrain law enforcement's ability to initiate the investigation and prosecution of those responsible for such offenses.

The bracketed language in the first paragraph creates the option of structuring the principle so that one must understand the risk she assumes, which is a traditional component of the tort principle.[200] If the principle as applied to criminal law is to achieve the desired result, however, it must impose strict liability.[201] The assumption of risk must arise from the act of venturing into cyberspace without having taken adequate precautions; knowledge of the risk being assumed should not be required because the purpose is to encourage citizens to educate themselves and to take measures to avoid risky behavior. Incorporating knowledge of the risk nullifies the efficacy of the principle without increasing the fairness of the result. The tort

[200] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 496C(1).

[201] *See* Brenner, *Toward a Criminal Law for Cyberspace: A New Model for Law Enforcement?*, *supra* note 3, at 89-104 (arguing that the criminal principle would operate differently for different classes of potential victims).

principle incorporates knowledge of the risk assumed because the consequence of assuming a civilly-defined risk is that the victim loses the right to seek financial redress for resulting injuries; requiring notice is therefore a matter of simple fairness.[202] In the cybercrime context, the victim loses the expectation of a law enforcement response; but since such an expectation may be unrealistic,[203] she actually "loses" nothing. Her assumption of a criminally-defined risk does not preclude her from seeking damages in a civil action against an appropriate party, nor does it preclude the apprehension and prosecution of the victimizer.[204] It merely negates the

[202] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 496D, cmt. b.

[203] *See supra* Part II(A)(3).

[204] Such a concept has been incorporated into at least some cybercrime statutes. Article 138a of the Dutch Criminal Code, for instance, states that one "who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, shall be liable, as guilty of breach of computer peace, to term of imprisonment" if he "[b]reaks through a security system" to gain access or "obtains access by a technical intervention, with the help of false signals or a false key or by acting in a false capacity." The Netherlands, Criminal Code, Article 38a, Cybercrime Law: A Global Survey of Cybercrime Legislation, http://www.cybercrimelaw.net/countries/netherlands.html (n.d.); According to a Dutch cybercrime expert, this provision incorporates assumption of risk so it is not a crime to access a Dutch computer system without authorization if the computer system was not secured. Conversation with Professor Bert-Jaap Koops, Senior Lecturer - Faculty of Law, Tilburg University, Netherlands, http://www.uvt.nl/websijs/english/show.html?anr=8225744&lang=en (n.d.);

A German statute has the same effect: "Any person who obtains without authorization … data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment . . . or to a fine." German Penal Code § 202a, http://www.cybercrimelaw.net/countries/germany.html (n.d.); Assumption of risk applies; "simple intrusion . . . is not punishable." Christian Schwarzenegger, *Computer Crimes in Cyberspace: A comparative Analysis of Criminal Law in Germany, Switzerland and Northern Europe* (2002), http://www.rwi.unizh.ch/schwarzenegger/person/pdf/ ComputerCrimeCyberSpace2002.pdf (n.d.)*; see also* Finnish Penal Code Chapter 38 § 8, Cybercrime Law: A Global Survey of Cybercrime Legislation, http://www.cybercrimelaw.net/countries/finland.html (n.d.). And assumption of risk is not unknown in this country*; see* N.Y. Penal Law § 156.05 (McKinney 2004) (one is guilty of unauthorized use of a computer when he knowingly and without authorization causes a computer to be used that "is equipped . . . with any device or coding system, a function of which is to prevent the unauthorized use of said computer").

supposition that one's victimization triggers an entitlement to an instantaneous and effective law enforcement response.

Implementing a principle such as this has both symbolic and pragmatic consequences. Symbolically, it emphasizes that citizens must protect themselves in cyberspace and cannot expect law enforcement to bring the perpetrator to justice if they are victimized. This confirms the already existing realities of cyberspace; police cannot, for example, seek justice for everyone who foolishly sends forty-five dollars for a Beanie Baby that was advertised on eBay but was never delivered (and probably never existed).[205] This brings us to the pragmatic consequences of adopting an online assumption of risk principle: Police and prosecutors know cases like the Beanie Baby example stand no chance of being "solved," yet they have no viable way to explain this to the public. In a culture that assumes the effectiveness of the reactive model of law enforcement, it would not be a wise career move for a county prosecutor to inform his constituents that if they are victimized in certain ways while online, his office will not pursue those cases. A modified assumption of risk principle such as the one set out above resolves this difficulty.

(b) Complicity[206]

Complicity doctrines are an appropriate choice for imposing responsibility to prevent cybercrime because they impute liability for another's criminal act to a non-actor (i.e. an

[205]*See e.g., Bidding in an Online Auction? Beware of Scams*, BUS. WK., Nov. 3, 1998, *available at* http://www.businessweek.com/bwdaily/dnflash/oct1998/sr81998/sr81103b.htm (woman paid $1,800 for a fake Beanie Baby)*; see also* Bob Sullivan, *Con Victims Out $10,000 or More*, MSNBC (Dec. 4, 2003), http://msnbc.msn.com/id/3660523/ (dentist who sent $55,000 to a face escrow site as payment for a BMW lost his money and never got the car).

[206]A more detailed treatment of this issue can be found in Brenner, *Distributed Security*, *supra* note 3.

accomplice) who facilitated that act.[207] Whereas the section above explains how a modified assumption of risk principle can be used to impose consequences for one's becoming a victim, this section considers how complicity doctrines can be used to impose liability for consequent victimization. Furthermore, while the previous section is concerned with imposing consequences for one's own victimization, this section is concerned with imposing liability for letting oneself become a victim of a cybercrime that is then used to victimize other individuals or entities.[208]

Under the theory of complicity, one who facilitates the commission of a crime can be held criminally liable for that crime, just as if he committed it himself.[209] Complicitous liability is usually based upon one's performing an affirmative act, though it can also be based upon inaction. Under the Model Penal Code, one is an accomplice if, having a legal duty to prevent a crime, she fails to do so;[210] this doctrine of complicity-by-omission has been used, for example, to hold parents liable for not preventing harm to their children.[211] Action or inaction alone is not enough. Most criminal codes require that an accomplice has acted with the purpose of facilitating the target crime.[212] In American law, while there is some authority for the proposition that accomplice liability can be imposed upon those who knowingly facilitate a

[207] *See, e.g.*, MODEL PENAL CODE § 2.06 (1962).

[208] *See supra* notes 198-204 & accompanying text.

[209] *See, e.g.*, MODEL PENAL CODE § 2.06(1) (1962).

[210] *See, e.g.*, MODEL PENAL CODE § 2.06(3)(a)(iii) (1962); *see also* WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 13.2(a) (2003) ("a conductor on a train might become an accomplice in the knowing transportation of liquor on his train for his failure to take steps to prevent the offense").

[211] *See, e.g.*, *State v. Tucker*, 861 P.2d 37, 43-44 (Haw. App. 1993).

[212] *See, e.g.*, MODEL PENAL CODE § 2.06(3)(a) (1962).

crime,[213] there is a general agreement that it cannot be based on reckless or negligent conduct.[214] Other codes are less lenient. For example, the statute governing the proceedings of the International Criminal Tribunal for the Former Yugoslavia imposes complicity-by-omission liability upon commanders who recklessly or negligently failed to prevent their subordinates from committing war crimes.[215]

The emphasis on "intention" found in the Model Penal Code and other domestic criminal codes is the product of two considerations. One is a concern that "otherwise everyday lawful activities would be made perilous";[216] for example, if negligence sufficed for complicity, selling lawful products could result in the imposition of criminal liability if those products were used to commit crimes. The other consideration is "the belief that people's freedom to act within the law should not be restrained by considerations of wrongs others might commit."[217] In other words, I should not be held liable for the intervening volitional act of one over whom I exercise no control. This is what differentiates the "command complicity" found in the statute governing the International Criminal Tribunal for the Former Yugoslavia from the codes that govern average citizens; civilians, unlike military commanders, generally do not have the authority to control the actions of others.[218]

---

[213] *See, e.g.*, WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 13.2(d) (2003); *Cf. United States v. Peoni*, 100 F.2d 401, 402-03 (2d Cir. 1938).

[214] *See, e.g.*, WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 13.2(e) (2003).

[215] *See, e.g.*, Mirjan Damaska, *The Shadow Side of Command Responsibility*, 49 AM. J. COMP. L. 455, 463-467 (2001); *see also Basic Statute of the International Criminal Tribunal for the former Yugoslavia*: *Report of the Secretary-General pursuant to paragraph 2 of S.C. Res. 808*, art. 7 ¶ 3 (1993), *available at* http://www.un.org/icty/legaldoc/index.htm.

[216] Stanford H. Kadish, *Reckless Complicity*, *supra* 87 J. CRIM. L. & CRIMINOLOGY at 382.

[217] *Id.* at 391.

[218] *See generally* Damaska, *supra* note 215, at 463-64.

Our goal in this undertaking is to craft rules which hold citizens responsible for preventing cybercrime. The assumption of risk principle outlined in the section above essentially negates any expectation of redress for one's own victimization; if I become the victim of a cybercriminal, I cannot expect that he will be brought to "justice" and be sanctioned. Yet, what if by allowing myself to be victimized I contributed to another's victimization? I have not only failed to protect myself, I have contributed to another's being harmed. I have, in effect, acted as an accomplice by engaging in conduct that facilitated the commission of a crime. Should we, therefore, use complicity-by-omission liability to hold me liable for this consequent victimization?[219] Such a step appears to be unacceptable because it (i) imposes omission liability in the absence of a legal duty to act;[220] and (ii) contravenes the two considerations noted in the paragraph above.[221] Nevertheless, with some modifications, complicity-by-omission liability could properly be used to impose liability.

The first, most problematic obstacle to recognizing complicity-by-omission liability is the conduct upon which liability is to be predicated. If we use the Model Penal Code's formulation of complicity, an omission cannot support the imposition of complicitous liability unless a duty to act is imposed by law. [222] We could, however, impose a legal duty to avoid becoming the victim of a cybercriminal.[223] In creating such a duty, we must resolve two issues:

---

[219]*See supra* Part II(C)(1).

[220]*See supra* note 210 and accompanying text.

[221]*See supra* notes 215 - 217 and accompanying text.

[222]*See supra* note 210 and accompanying text.

[223]Since such a duty did not exist at common law, it would have to be statutorily imposed. This could be done *seriatim*, by having states adopt laws to this effect; it might be possible to enact such a duty at the federal level, given the deleterious effects cybercrime and cyberterrorism have upon interstate commerce. *See generally* Joseph P. Bauer, *The Erie Doctrine Revisited: How A Conflicts Perspective Can Aid the Analysis*, 74 NOTRE DAME L. REV. 1235, 1243 n. 34 (1999); Another possibility, using the Model Penal Code's approach to complicity, would be to

(i) the scope of the duty; and (ii) the extent of the obligation one bears in discharging it. As to the scope of the duty, it is sufficient to limit it to preventing one's own victimization; letting myself be attacked is how I contribute to the victimization of others.[224] This limited duty is sufficient because if I protect my computer from attack, I prevent its being used to attack others; conversely, if I do not protect my computer from attack, I have created at least the possibility that it could be used to attack others.[225] If a cybercriminal takes advantage of the opportunity I have supplied, it is reasonable to hold me liable, at least to some extent, for resulting cybercrimes. As to the obligation one has to discharge this duty, the most reasonable approach is to incorporate a negligence standard.[226] Strict liability would only undermine the incentive to take precautions, since one would be held liable for consequent victimization regardless of the efforts he took to avoid being personally victimized.[227] Under a negligence standard, liability would be imposed for failing to take the precautions a reasonable person would have known were necessary to protect the system(s) at issue.[228] The determination as to whether particular

---

declare that the failure to prevent a cybercrime which results in the victimization of others is itself enough to establish complicity. *See* MODEL PENAL CODE § 2.06(3)(b) (1962) (one is an accomplice if "his conduct is expressly declared by law to establish his complicity").

[224]It is also possible that I can be victimized as the result of my own gullibility, i.e., as the result of succumbing to "social engineering" and other tactics.

[225]*See, e.g.*, Adrian McCullagh, *Management Responsibility in Protecting Information Assets: An Australian Perspective*, 7 FIRST MONDAY (July 2002), *at* http://www.firstmonday.dk/issues/issue7_7/mccullagh/index.html#m5, (last visited September 25, 2004) (arguing that organizations should have a positive duty, enforceable by criminal liability, to prevent their computer systems from being used as zombies in a distributed denial of service attack).

[226]*See, id.*

[227]*See, e.g.*, WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 5.5(c) (4th ed. 2003).

[228]*See* MODEL PENAL CODE § 2.02(2)(d). A negligence standard would encompass reckless, knowing and purposeful failures to carry out the duty to prevent personal victimization. *See id.* at § 2.02(5). As to the type of precautions it would be "reasonable" to take, *see, e.g.*, McCullagh, *supra* note 225.

measures were necessary would have to include a temporal element, that is, it would have to focus on contemporaneously available security measures.[229]

Imposing such a duty is in a sense implementing a "do" rule under the scheme outlined above;[230] it imposes an affirmative obligation to implement security measures to fend off attacks by cybercriminals and imposes liability for not discharging this obligation. The duty outlined here differs from a "do" rule, however, in that liability is not imposed for the mere failure to discharge the specified duty.[231] If someone becomes the victim of a cybercrime, she will not be held liable as an accomplice to her own victimization;[232] she will only be deemed to have assumed the risk of her victimization. Criminal liability based upon complicity is only imposed if she fails to discharge her duty to protect herself and thereby contributes to the victimization of another. This result is consistent with traditional principles of criminal liability because the victim is being sanctioned not for being a victim but for playing a causal role in the commission of a crime against someone else.[233]

That brings us to the second consideration: the considerations which dictate that accomplice liability must be based on purposeful or at least knowing conduct.[234] We begin with the second consideration: if we do not require purpose or at least knowledge, we risk holding

[229]It might also be advisable to incorporate the type of user into the standard so that, for instance, corporate entities are held to a higher level than individual, home users of computer technology.

[230]*See supra* Part II(A)(4)(b).

[231]*See supra* note 210 and accompanying text.

[232]*See* MODEL PENAL CODE § 2.06(6)(a) (victim is not generally an accomplice).

[233]*See, e.g.*, Anick Jesdanun, *Digitally informed: Should a license be required to go online?*, DETROIT NEWS, September 12, 2003, *at* http://www.detnews.com/2003/technology/0309/14/technology-268979.htm, (last visited September 25, 2004) (Oberlin College threatens students to fine students who inadvertently spread a virus). *See also* Anne C. Paine, *CIT Wages War against Potent Virus and Wins*, OBERLIN ONLINE, September 12, 2003, *at* http://www.oberlin.edu/news-info/03sep/computerVirus.html, (last visited September 25, 2004) ("any student whose computer was found to be the source of a virus would be fined $25").

[234]*See supra* notes 216 - 218 and accompanying text.

citizens liable for the volitional acts of those over whom they have no control.[235] For example, liability without a knowledge requirement would encompass the following scenario: Cybercriminal (X) victimizes A and then uses his victimization of A to consummate his victimization of B (and C and D and so on).[236] It may seem unreasonable to hold A liable for this cyber-miscreant's attacks on B (and C and D and so on).[237] Assuming the most challenging scenario,[238] in which A does not know X, A has no control over X, and A was merely negligent in not preventing X's gaining access to his computer, it seems that we would be holding A liable for nothing more than failing to prevent a stranger from attacking other strangers. Arguably, this is as unreasonable as holding a liquor store clerk liable as an accomplice if a customer to whom she sold a bottle of whiskey uses it to incapacitate a young woman whom he rapes or to enter a state of gross intoxication during which he batters his wife to death.[239] Nonetheless, these two scenarios do in fact differ in at least one important respect. In the second scenario, the liquor store clerk is held liable for the volitional and consequently unforeseeable acts of her customer, based on her having sold him a product; her conduct was lawful and she has neither the right nor

[235]*See supra* note 216 and accompanying text.

[236]The scenarios discussed above assume that X uses A's computer as the vector from which to launch attacks on others; it is also possible that A contributes to the victimization of others by falling prey to "social engineering" and comparable tactics.

[237]If we require that A have acted with the purpose of facilitating X's attacks or that he knew his default would facilitate X's attacks, we establish a connection between the two that makes it reasonable to impute liability for X's actions to A.

[238]Other scenarios would involve instances in which A knew that he might be subject to an attack from X or in which A exercised some control over X, perhaps as X's employer where A knows X has a predilection for cyber-misconduct.

[239]Civil liability can be imposed for selling statutorily-controlled products, such as weapons and ammunition, to minors. *See* Robert M. Howard, Note, *The Negligent Commercial Transaction Tort: Imposing Common Law Liability On Merchants For Sales And Leases To 'Defective' Customers*, 1998 DUKE L.J. 755, 758 (1998). The only avenue for imposing criminal liability is simplicity.

the ability to control what he does after he leaves the store. In the first scenario, however, A is held liable not for failing to control X (which is impossible given that A does not know X and has no authority to control X's actions) but for failing to prevent equipment and processes that are within A's control from being attacked and compromised to the detriment of others. We cannot hold A liable for what X does on the theory that A should have prevented X from attacking others; but we can hold A liable for giving X access to the tools he needed to victimize others, thereby defaulting on his legal duty to prevent his computer system from being compromised.[240] Applying the second theory to this scenario is consistent with traditional accomplice liability because A is held liable for contributing to the success of the criminal venture.

Some may still find this outcome unpalatable because it can result in A's being held liable for a sequence of cybercrimes that X committed against B (and C and D and so on).[241] This undeniably harsh result could be alleviated by only holding A liable as a facilitator of those crimes, and not as an accomplice to X's cybercrimes.[242] New York and other states have recognized a separate "criminal facilitation" offense, whereby one who provides another with the

[240]An imperfect source of analogy, perhaps, are laws that hold a parent liable for not preventing a child from obtaining access to a weapon and using it to commit a crime**.** In *State v. Wilchinski***,** a father was charged with criminally negligent storage of a firearm after his son found his gun and used it to kill another child. 700 A.2d 1, 3 (Conn. 1997). He claimed that the negligent storage statute held gun owners liable "for the acts of another without requiring the state of prove that the owner was an accessory" under the state complicity statute, which limits accomplice liability to affirmative acts taken to facilitate a crime. *Id.* at 12. The Connecticut Supreme Court disagreed: "[T]he offense…is not the resulting injury or death but…the improper storage of the weapon that lead to the tragedy." *Id.*

[241]*See* MODEL PENAL CODE § 2.06(1).

[242]*See, e.g.*, Office of New York State Attorney General Eliot Spitzer, *Breakthrough Cited In War Against Child Porn*, February 16, 2001 *at* http://www.oag.state.ny.us/press/2001/feb/feb16c_01.html (last visited September 25, 2004) (Buffnet, an Internet Service Provider pled guilty to criminal facilitation of child pornography).

means or opportunity to commit a crime can be held liable as a facilitator of that crime.[243] The difference between criminal facilitation and accomplice liability is that the facilitator is not held liable for the crimes she promoted; she is, instead, held liable for criminal facilitation, a separate and often relatively minor offense.[244] A two-tiered system is therefore the best way to alleviate the potentially harsh consequences of imputing liability on the basis of negligent conduct: While criminal facilitation liability could be used for those who negligently contribute to consequent victimization (with sanctions limited to a fine or perhaps a fine coupled with a restriction on computer use), [245] accomplice liability would be reserved for those who purposefully or knowingly further the commission of cybercrimes.[246]

2. "Architects"

> *`The broad issue is, as a matter of policy, do we want suppliers of products and systems that are critical to our economy to be able to absolve themselves of all liability. . . .'*[247]

Since the real-world is not a human artifice, the notion of imposing criminal liability on the "architects" of cyberspace raises issues we have not yet had occasion to address.[248] The first issue we need to consider is the posture these "architects" occupy as to cyberspace. Are they, in effect, the "manufacturers" of cyberspace such that it would be logical and reasonable to hold

---

[243]*See, e.g.*, N.Y. PENAL LAW §§ 115.00, .01, .05, .08 (2003). *See also* note 239.

[244]*See, e.g.*, LAFAVE, *supra* note 227, § 13.2(d). *See also* note 243.

[245]*See, e.g.*, ARIZ. REV. STAT. § 13-1004 (2004).

[246]*See, e.g.*, Computer Crimes Act, Malaysia Act 563.7 § 7(1) ("abetments . . . punishable as offences"), *available at* http://www.geocities.com/Tokyo/9239/comcrime.html (last visited September 16, 2004).

[247]Steve Lohr, *Product Liability Lawsuits are New Threat to Microsoft*, N.Y. TIMES, October 6, 2003, at C2. (quoting Mark D. Rasch), http://www.lexisone.com/news/n100603a.html, (last visited September 27, 2004).

[248]*See supra* Part II(B).

them liable for security lapses under a product liability theory?[249] Are they providers of services as to whom such lapses could be considered malpractice?[250] Are they both? Neither?

The resolution of these questions requires re-examining the rationale for imposing criminal liability on "architects." As explained earlier, the rationale derives from the system of distributed security which shifts the focus of maintaining order in cyberspace from *reacting* to cybercrime to *preventing* cybercrime and assigns responsibility for preventing cybercrime to citizens.[251] Since we concluded that we cannot rely upon voluntary participation if such a system is to be effective,[252] we must require preventative efforts. Part II(C)(1) outlined the requirements to be imposed upon "users." Similar requirements should be imposed upon "architects," because of the role they play in the collective experience we know as cyberspace. "Architects" supply the devices – hardware and software – that "users" employ to participate in cyberspace;[253] consequently, these "architects" are uniquely equipped to determine the reliability and technical adequacy of these devices. Since the efficacy with which "users" can avoid cybercrime is a function of the reliability and technical adequacy of the tools they employ, "architects" are in a position to enhance the overall effectiveness of the system of preventative,

[249]*See e.g.*, Jody Armour & Watts S. Humphrey, *Software Product Liability*, SOFTWARE ENGINEERING INSTITUTE, August 1993, *available at* http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr13.93.pdf (last visited September 16, 2004).

[250]*See e.g., From the Editor*, SOFTWARE QUALITY PROFESSIONAL, March 2002, http://www.asq.org/pub/sqp/past/vol4_issue2/editor.html (last visited October 20, 2004) ("One sign of the maturing of our profession would be a wider acceptance of the concept of 'software malpractice'.").

[251]*See supra* Parts II(A)(4) and II(B). Citizen responsibility is certainly not the only device that will be used to prevent cybercrime, but it is very important. *See id.*

[252]*See supra* Part II(A)(4)(b).

[253]*See supra* Part II(B).

distributed security postulated here by enhancing the reliability and adequacy of these tools.[254] Unfortunately, they have not taken advantage of this opportunity; software vulnerabilities and other defects in the infrastructure of cyberspace continue to be facilitating factors for cybercriminals.[255]

Generally, the prospect of product liability claims creates incentives for manufacturers to ensure that products are safe and defect free;[256] the same is not true, however, for the "architects" of cyberspace:

---

[254]*See, e.g., Cyberattacks and Cyberterrorism: What Private Business Must Know*, GARTNER G2, September 25, 2002, *available at* http://www.gartnerg2.com/qu/qu-0902-0091.asp ("[S]oftware manufacturers have to improve the security and reliability of their products" if businesses an other users of cyberspace are to avoid cybercrime.).

[255]*See, e.g.,* William Yurcik & David Doss, *CyberInsurance: A Market Solution to the Internet Security Market Failure*, WORKSHOP ON ECONOMICS AND INFORMATION SECURITY, 2002, *at* http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/53.pdf. (last visited September 16, 2004):

> The poor state of security on the Internet is the direct result of a market failure. Software companies have been able to institute a framework denying them liability for faulty products. In addition, time-to-market . . . pressures compel software companies to release software as early as possible with lower levels of testing, if any testing at all. This combined with the increasing complexity of software virtually ensures the software flaws will exist that will be exploited as security vulnerabilities . . . .[T]here is little or no incentive for a software manufacturer to be responsive in developing . . . and distributing patches for software vulnerabilities in their products.

See also Madeline Bennet, *Interview: Microsoft Wages War on Flaws*, VNUNET, December 5, 2002, *at* http://www.vnunet.com/Features/1137383 (last visited September 29, 2004) ("`if you do a degree in computer science, you are not taught how to write secure code . . . . [T]esters simply look at whether product does what it is supposed to do'"); Dinah Greek, *The Real Impact of Viruses: Part 1*, VNUNET, January 6, 2004, *at* http://www.vnunet.com/Features/1151775 (last visited September 29, 2004)("Over 1,400 new software vulnerabilities are discovered every week. . . .").

[256]*See e.g.* Gerald F. Tietz, *Strict Products Liability, Design Defects and Corporate Decision-Making: Greater Deterrence Through Stricter Process*, 38 VILL. L. REV. 1361, 1365 (1993) ("Courts and commentators . . . agree that . . . products liability creates incentives for manufacturers to ensure greater product safety.")*; see also* AMERICAN LAW OF PRODUCTS LIABILITY 3d § 1:1 (2004):

> Software manufacturers are the favored sons of contract, product liability and tort law: the economic loss doctrine limits damages against software vendors to the terms of the license, usually to the price of the software itself. The underlying rationale . . . is the `concern that product liability claims could circumvent the objectives of the [Uniform Commercial Code].'[257]

> Products liability law . . . refers to the legal responsibility for injury resulting from the use of a product. The paradigmatic products liability action is one in which a product causes bodily harm and the manufacturer is held liable . . . because of public policy which demands that responsibility be fixed wherever it will most effectively reduce the hazards to life and health inherent in defective products. . . . [T]he term . . . typically covers any liability of a manufacturer or other distributer of a product where personal injury or damage to some other property is caused by a defect in the product.

[257]Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability and The First Amendment*, 24 WHITTIER L. REV. 71, 134 (2002) (quoting Steven C. Tourek, et al., *Bucking the "Trend": The Uniform Commercial Code, the Economic Loss Doctrine, and Common Law Causes of Action for Fraud and Misrepresentation*, 84 IOWA L. REV. 875, 887 (1999)). *See e.g.* Declan McCullagh, *A Legal Fix for Software Flaws?*, ZDNET, August 26, 2003, *at* http://www.zdnet.com/2100-3513_22-5067873.html (last visited September 16, 2004); Charles C. Mann, *Why Software Is So Bad*, TECHNOLOGY REVIEW, 33, 38 (July/August 2002), *at* http://www.thesmallworlds.com/pres/WhySoftwareIsSoBad.pdf*; see also* Steve Lohr, *Product Liability Lawsuits are New Threat to Microsoft*, N.Y. TIMES, October 6, 2003, at C2, http://www.lexisone.com/news/n100603a.html, (last visited September 27, 2004)('[S]oftware companies have sidestepped liability . . . by selling customers a license to use their programs . . . with a lengthy list of caveats and disclaimers"). The economic loss doctrine is

> a judicially created doctrine under which a purchaser of a product cannot recover from a manufacturer on a tort theory for damages that are solely economic . . . It is based on an understanding that contract law . . . is better suited than tort law for dealing with purely economic loss in the commercial arena . . . Therefore, when . . . the only damages are economic losses, the exclusive remedy lies in contract. . . .
>
> In contract law, the parties' duties arise from the terms of their . . . agreement; the goal is to hold parties to that agreement so that each receives the benefit of his or her bargain. The aim of tort law . . is to protect people from misfortunes which are unexpected and overwhelming. The law imposes tort duties upon manufacturers to protect society's interest in safety from the physical harm or personal injury which may result from defective products. Thus, where a product fails in its intended use and injures only itself, thereby causing only economic damages to the purchaser, 'the reasons for imposing a tort duty are weak and those for leaving the party to its contractual remedies are strong.'

Many find this apparent bias to be intolerable. As a National Academy of Sciences Report noted, software companies "use customers as implicit beta testers to shake out security flaws" in their products.[258] In response, software industry executives argue that the imposition of such liability is inappropriate because "software is a highly complex product, often misused or modified by consumers" and because the software industry is "a fast-changing global business . . . led by United States companies. Opening the industry up to product liability lawsuits . . . would chill innovation and undermine the competitiveness of American companies."[259] Other obstacles to using product liability or similar civil doctrines to improve the reliability of software include the lack of standards of reliability for software; the fact that companies tend not to want to pay the higher costs associated with more reliable software; and that consumers often fail to recognize the potential security flaws inherent to the software.[260]

These issues and arguments, however, all deal with *civil* product liability. The focus of this article is on using criminal liability to implement a system of distributed security to prevent cybercrime. Could a doctrine of *criminal* product liability be used for this purpose? Could criminal liability be used to hold the "architects" of cyberspace liable for defects in software and hardware that contribute to the commission of cybercrimes? While such an approach is

---

Bay Breeze Condo. Ass'n v. Norco Windows, Inc., 651 N.W.2d 738, 741-42 (Wis. Ct. App. 2002)(quoting Wausau Tile Co. v. County Concrete Corp., 593 N.W.2d 445, 451-52 (Wis. 1999)).

[258]NATIONAL ACADEMY OF SCIENCES-COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, CYBERSECURITY TODAY AND TOMORROW 13 (2002), http://books.nap.edu/html/cybersecurity/ch1.html (last visited September 29, 2004).

[259]Lohr, *supra* note 257.

[260]*See, e.g.*, Brian Robinson, *Making Software NASA-Tough*, FEDERAL COMPUTER WEEK (July 1, 2002), http://www.fcw.com/fcw/articles/2002/0701/tec-nasa-07-01-02.asp (last visited September 16, 2004); *Spread of Buggy Software Raises New Questions*, ACCORDSQA, http://www.accordsqa.com/news/030427-buggysoftware.html (last visited October 20, 2004)*; see also* Gregory Tassey, *The Economic Impacts of Inadequate Infrastructure for Software Testing*, 2002 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY E1-E5, http://www.nist.gov/director/prog-ofc/report02-3.pdf.

consistent with holding "users" criminally liable for failing to prevent cybercrime, it is inconsistent with both the reluctance to apply civil product liability to software and the United States' lack of general criminal product liability.[261] The sections below consider the advisability and implications of such a measure.

(a) Civil Products

In the United States, the doctrine of product liability evolved in the context of civil tort litigation between consumers and manufacturers: "[P]roducts liability doctrines . . . developed to give manufacturers incentives to design safer products by providing a cause of action to injured consumers."[262] The law and doctrines of product liability therefore assume "civil" products; that is, they assume product liability litigation involves a private plaintiff, whether individual or corporate, seeking redress for injuries and/or damages resulting from defects in a product that is used solely in a "private" capacity.[263] In one sense, this is true of the software and hardware that are used to constitute and sustain cyberspace; in another, it is not.

The previous arguments as to why product liability law should not be applied to computer hardware and software implicitly assume that both represent "civil" products that are used in a purely "private" capacity by individuals and commercial entities. This assumption is not in dispute. I am writing this article on my personal laptop using Microsoft software. If my

[261] As to the latter, *see infra* note 269.

[262] Mark D. Oshinskie, *Tanks for Nothing: Oil Company Liability for Discharges of Gasoline from Underground Storage Tanks Divested to Station Owners*, 18 VA. ENVTL. L.J. 1, 23 (1999). *See also* Victor E. Schwartz & Rochelle M. Tedesco, *The Re-Emergence of "Super Strict" Liability: Slaying the Dragon Again*, 71 U. CIN. L. REV. 917, 926 (2003) ("Product liability . . . developed . . . in response to the deficiencies in the rights of action available to consumers' negligence and warranty") (quoting George L. Priest, *Strict Products Liability: The Original Intent*, 10 CARDOZO L. REV. 2301, 2305 (1989).

[263] Addison v. Williams, 546 So. 2d 220, 223 (La. Ct. App. 1989) ("This case does not involve issues of 'gun control.' This is a civil damage suit between private parties to be decided . . . under products liability law.").

laptop suffered a catastrophic system failure and shocked me with high-voltage electricity, or if the software had a meltdown and deleted this article and the files I have compiled over the last decade, I could try suing the laptop manufacturer for my physical injuries or Microsoft for the loss of my data. Under current law, I might be able to recover for my physical injuries, but I could not recover for the loss of my data; product liability law would probably apply to the defective laptop that caused physical injury, but it certainly would not apply to the software and its failure.[264] As explained earlier, [265] the software industry has successfully argued that (i) product liability is inadvisable for a "product"/"service" as complex and subject to misuse as software; and (ii) imposing product liability would stifle innovation and thereby undermine America's superiority in this area. As a result, product liability law today remains inapplicable to the software itself and any damages it causes.

Although the software industry's two main arguments are objectionable on various grounds, their merits are irrelevant to the issues under consideration in this article because both assume *civil* product liability. That is, both arguments assume that the imposition of product liability would have a deleterious effect upon the software industry's ability to conduct business because it would have to deal with thousands of civil lawsuits brought by dissatisfied "private" users of its products. This deleterious effect would presumably derive from various factors, such as the time, effort and expense required to defend these actions or the difficulties attendant upon accommodating inconsistent legal standards imposed by different states or nations. Under consideration here, however, is the use of a doctrine of criminal product liability; criminal actions are brought not by any consumer who happens to be dissatisfied with a product, but by

[264]*See* Part II(C)(2), *supra;* Laurel M. Cohn, *Products Liability: Computer Hardware and Software*, 59 A.L.R. 461 (1998). *See also supra* note 257.

[265]*See* Part II(C)(2), *supra.*

the state, which must have probable cause to believe a crime has been committed. Requiring probable cause, without more, limits the number of cases that are filed and tends to avoid frivolous litigation. It is also possible, as Part II(C)(2)(b) explains, to control the imposition of such liability by structuring the mechanisms used to initiate cases so that they restrict the number of prosecutions filed, e.g., by providing opportunities for case review, diversion and settlement.

The first argument the software industry advances as to why product liability law should *not* be applied to software actually supports the converse proposition that criminal product liability *should* be imposed. The software industry's arguments not only assume *civil* product liability, but also that software is a "civil" product. As such, software is functionally indistinguishable in an important respect from other products that are used in a purely "private" capacity by individuals and entities and as to which product liability is imposed. This argument, as applied to my laptop's data loss scenario described above, assumes that my laptop and the software I use are discrete products indistinguishable from other household goods, such as my toaster or my stereo. In other words, the industry's argument assumes that the laptop and the software are items that have distinct functions and that I employ them for purely "private" use. It also assumes that any defect which causes the laptop or the software to fail is purely a private matter to be resolved between the manufacturer and myself. These assumptions are incorrect because software, in particular, is no longer a "civil" product. Due to its role in creating and sustaining the complex communicative experience we know as cyberspace, software has become an essential component of our national infrastructure[266] and its importance will only increase as

[266]*See, e.g.,* Office of the President, *The National Strategy to Secure Cyberspace* 32-33 (February 2003), http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf:

more and more activities (private, government, commercial, educational, scientific, etc.) move into cyberspace. [267] As an increasingly important component of our national (and international) infrastructure, software is too important to be left to the vagaries of "private" civil litigation. We must devise some system for ensuring that the software providers upon whom we rely are taking adequate measures to ensure that the software we use is reliable and technically adequate.[268]

> A . . . critical area . . . is the many flaws . . . in critical infrastructure due to software vulnerabilities. . . . [A]pproximately 3,500 vulnerabilities are reported annually . . . . Unpatched software in critical infrastructures makes those infrastructures vulnerable to penetration and exploitation. Software flaws are exploited to propagate 'worms' that can result in denial of service, disruption, or other serious damage. Such flaws can be used to gain access to and control over physical infrastructure . . . .

See also id. at 1:

> Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures. . . . [T]he healthy functioning of cyberspace is essential to our economy and our national security.

[267]*See, e.g., id.* at 6:

> By 2003, our economy and national security became fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping . . . .

See also Charles C. Mann, *Why Software Is So Bad*, TECHNOLOGY REVIEW, 33, 38 (July/August 2002), *at* http://www.technologyreview.com/purchase/pdf_dl.asp?70juh=115185&hy6f0=4998.

[268]*See, e.g.*, Rich Mogull & Richard Hunter, *Cyberattacks and Cyberterrorism: What Private Business Must Know* (2002), *at* http://www.gartnerg2.com/qa/qa-0902-0091.asp ("Software is currently exempt from product liability laws, removing any possible legal recourse for unacceptable quality. Software manufacturers must be held to an appropriate standard of quality, like all other commercial products.") (on file with the author); Computer Science and Telecommunications Board - National Academy of Sciences, Computer Security: Today and Tomorrow 14 (2002), *at* http://books.nap.edu/html/cybersecurity/ch1.html ("Policy makers should . . . [c]onsider legislative responses to the failure of existing incentives to cause the market to respond adequately . . . .Possible options

Employing criminal liability for this purpose is not without precedent in this country.[269] In certain respects, it is analogous to the imposition of liability for antitrust violations.[270] Antitrust enforcement can consist of either civil or criminal proceedings.[271] Since the focus of this article is on criminal liability, we will restrict our consideration of antitrust to criminal enforcement proceedings.[272] Criminal antitrust proceedings differ from traditional crimes in a notable respect: Criminal antitrust proceedings are predicated on the infliction of a systemic "harm," whereas traditional criminal proceedings are predicated on the infliction of "harm" to individual victims, whether humans or artificial entities.[273] In a traditional criminal proceeding, the state acts to vindicate its obligation to protect the individual members of the

---

include steps that would increase the exposure of software and system vendors . . . to liability for system breaches and mandated reporting of security breaches . . . . ") (on file with the author).

[269]While criminal product liability, as such, is not an element of American law, other countries do hold the manufacturers and distributors of defective products criminally liable for their actions. *See, e.g.*, People's Republic of China - Standing Committee of the Eighth National People's Congress, Decision of the Standing Committee of the National People's Congress on Punishing the Crimes of Production and Sale of Fake or Substandard Commodities ¶ 5 (July 2, 1993) *at* http://www.lehmanlaw.com/lib/library/Laws_regulations/consumer/decision.htm (criminal offense to produce or sell "products that do not conform to the national or trade standards safeguarding the safety of person or property") (on file with the author). *See also* Commonwealth of Australia, Trade Practices Act of 1974 § 75AZS (1974) *at* http://www.austlii.edu.au/au/legis/cth/consol_act/tpa1974149/s75azs.html (on file with the author); United Kingdom Department of Trade and Industry, Country Report: Italy, *at* http://www.dti.gov.uk/ccp/topics1/pdf1/benchitaly.pdf (on file with the author).

[270]The software industry has, of course, been the target of antitrust proceedings. *See* U.S. Department of Justice – Antitrust Division, United States v. Microsoft, *at* http://www.usdoj.gov/atr/cases/ms_index.htm (on file with the author).

[271]*See, e.g.*, Raymond Krauze & John Mulcahy, *Antitrust Violations*, 40 Am. Crim. L. Rev. 241, 241-243 (2003).

[272]*See id.* at 269-279. *See also* U.S. Dept. of Justice: United States Attorneys' Manual § 7-5.000 (1997) *at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title7/5mant.htm (on file with the author).

[273]For the proposition that laws defining "crimes" target the infliction of discrete types of "harm," *see, e.g.*, Part II(A)(1), *supra. See also* Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 Cal. Crim. L. Rev. 1 (2001) *at* http://boalt.org/CCLR/v4/v4brenner.htm (on file with the author).

social system it represents;[274] in a criminal antitrust enforcement proceeding, however, the state acts to vindicate its obligation to ensure the viability of an essential component of a social system. The "harm" caused by an antitrust "crime" is an erosion of the principle of competition: "[F]ree and competitive markets result in maximum economic development, wealth creation, and consumer welfare, but . . . markets will not always remain free and competitive in the absence of effective government oversight."[275] Criminal antitrust proceedings therefore target "systemic" crimes, i.e., crimes that impact upon a nation's infrastructure instead of upon its individual citizens,[276] and are in that regard precisely analogous to the type of criminal liability postulated here. Like criminal antitrust laws, criminal product liability laws would authorize the imposition of liability upon those whose conduct undermines the security of the national infrastructure.[277]

Though criminal antitrust proceedings are analogous insofar as they target systemic injury, they differ in another respect: They require affirmative "criminal" conduct.[278] The context-specific criminal product liability postulated here, on the other hand, would be imposed

---

[274]*See, e.g.*, ABA STANDARDS FOR CRIMINAL JUSTICE 3-2.1, Commentary (1994).

[275]Joel I. Klein, Rethinking Antitrust Policies for the New Economy, Address at the Haas/Berkeley New Economic Forum, University of California at Berkeley (May 9, 2000) *at* http://www.usdoj.gov/atr/public/speeches/4707.htm (on file with the author). *See also* U.S. Dept. of Justice: United States Attorneys' Manual § 7-1.100 (1997) *at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title7/1mant.htm ("The U.S. antitrust laws represent . . . our nation's commitment to a free market economy in which the competitive process of the market ensures the most efficient allocation of our scarce resources and the maximization of consumer welfare.") (On file with the author).

[276]Charles S. Stark, *International Cooperation in the Pursuit of Cartels*, 6 Geo. Mason L. Rev. 533, 533 (1998) ("antitrust . . . enforcement . . . is very much a part of the global economic infrastructure").

[277]*See supra* notes 266 - 268 and accompanying text.

[278]*See, e.g.*, U.S. Dept. of Justice: United States Attorneys' Manual § 7-1.100 (1997) *at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title7/1mant.htm (antitrust laws target "private restraints of trade (such as price fixing, bid rigging and other collusive arrangements among competitors) that unreasonably impede the free forces of the market").

for inaction, i.e., for not ensuring the reliability of software or hardware.[279] The imposition of such liability is not unknown in American law; there are sources of analogy for holding one criminally liable for failing to prevent "harm," including systemic "harm."[280] In *United States v. Park,*[281] for instance, a corporate officer was convicted of violating 21 U.S.C. § 331(k), which makes it a federal crime to let food shipped in interstate commerce and held for sale to become adulterated.[282] Park was the president of a "national retail food chain" that used a Baltimore warehouse to store food which had been shipped in interstate commerce and was being held for sale to consumers.[283] Federal inspectors determined that the warehouse was "accessible to rodents" and that the rodents were contaminating the food stored there; this contamination

---

[279]*See supra* Part II(C)(2). We do not need criminal product liability to address the conduct of one who intentionally or knowingly distributes a defective product that can cause "harm" to citizens or to a social system. *See, e.g.,* Michael Rustad & Thomas Koenig, *Historical Continuity Of Punitive Damages Awards: Reforming The Tort Reformers,* 42 Am. U. L. Rev. 1269, 1329 n. 296 (1993) ("first American prosecution of a manufacturer for manslaughter arose from three deaths caused by the . . . defective Ford Pinto. . . . The prosecutor based the case on the company's failure to recall a potentially deadly vehicle when the company had knowledge of a defect in the vehicle"). *See also* Michael B. Metzger**,** *Corporate Criminal Liability for Defective Products: Policies, Problems, and Prospects*, 73 Geo. L.J. 1, 3 (1984).

[280]*See, e.g.,* United States v. FMC Corp., 572 F.2d 902 (2d Cir. 1978) (corporation convicted of failing to prevent the deaths of migratory birds under 16 U.S.C. § 703). The imposition of criminal liability for one's failure to prevent a particular type of generalized, systemic "harm" dates back to the beginning of the twentieth century and the invention of "public welfare" offenses. *See* Francis B. Sayre, *Public Welfare Offenses*, 33 Colum. L. Rev. 55, 67-68 (1933). The development of "public welfare," or regulatory, offenses resulted from a "shift in emphasis from the protection of individual interests which marked nineteenth century criminal administration to the protection of public and social interests." M. Diane Barber, *Fair Warning: The Deterioration Of Scienter Under Environmental Criminal Statutes,* 26 Loy. L.A. L. Rev. 105, 110 (1992). *See also* Sayre, *Public Welfare Offenses, supra*, 33 Colum. L. Rev. at 67-68.

[281]421 U.S. 658 (1975).

[282]*See* 421 U.S. at 660. *See, e.g.,* 21 U.S.C. § 331(k). *See also* U.S. Department of Justice: United States Attorneys' Manual Title 4 § 104 (1998) *at* http://www.usdoj.gov/usao/eousa/foia_reading_room/ usam/title4/civ00104.htm (elements of an offense under the Food, Drug and Cosmetic Act, 21 U.S.C. § 301 *et seq.*) (on file with the author).

[283]*See* 421 U.S. at 660.

constituted adulteration under 21 U.S.C. § 331(k).[284] Park and the company were charged with violating § 331(k), and the company pled guilty. Park, however, pled not guilty.[285] Park claimed that he was not "personally responsible" for the contamination at the Baltimore warehouse.[286] He conceded that while all of the company's employees "were in a sense under his general direction," the responsibility for ensuring sanitary conditions at the warehouse belonged to the Baltimore division vice president. Park further claimed that he had checked and was told the vice president was taking "corrective action."[287] Notwithstanding that claim, Park was convicted; he subsequently appealed to the United States Supreme Court. The Court upheld his conviction, concluding that Park's "responsible" position in the company's corporate structure justified holding him liable for failing to prevent the contamination.[288]

The *Park* case highlights an issue that is of central importance in crafting a doctrine of criminal product liability encompassing software and hardware used to access cyberspace: What, if any, *mens rea* should be required for the imposition of liability? As seen in the *Park* case and in other areas of real-world criminal law, strict liability is sufficient.[289] Note, however, that in crafting the "user" complicity rule, we rejected strict liability in favor of a negligence standard.[290] The resolution of this issue depends upon how we characterize the type of liability that is being imposed: Is it liability for committing a traditional "crime" or is it the less onerous liability imposed for committing a regulatory offense?

---

[284]*See id.*

[285]*See id.* at 661-62.

[286]*See id*. at 662-63.

[287]*See id*. at 663-64.

[288]*See id*. at 668-70.

[289]*See id. See, e.g.*, United States v. FMC Corp., 572 F.2d 902 (2d Cir. 1978). *See also* Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 13.5 (2003).

[290]*See supra* Part II(C)(1)(b).

Strict liability suffices in cases like *Park* because the corporation or the corporate employee is being held liable not for a traditional crime, but for a regulatory offense, i.e., for violating a statute that "impose[s] a duty upon the corporation not to act in such a way as to endanger the health, safety or welfare of the general public."[291] Strict liability is used because it can be difficult, if not impossible, to prove personal moral fault on the part of specific corporate employees; further, as the advocates of strict liability note, the penalties associated with regulatory offenses are usually small, often consisting of only a fine.[292]

We rejected strict liability for the "user" complicity rule because we concluded that it would be ineffective and because it would impose liability for the commission of a traditional "crime."[293] Under the complicity rule, a "user" who fails to prevent his computer from being compromised and used to victimize another is held liable either as an accomplice to the crimes committed or for the separate offense of facilitation.[294] The penalties imposed upon an accomplice can be severe. While the penalties for facilitation are generally less severe, a conviction still represents a conviction for a traditional "crime," not for a regulatory offense.[295]

Thus, the most reasonable strategy for crafting a criminal product liability principle applicable to the "architects" of cyberspace is to define a regulatory offense based on strict

---

[291]LAFAVE, *supra* note 23, at § 13.5 (C).

[292]*See, e.g,, id*. at § 5.5 (C). *See also Park*, 421 U.S. at 661-62.

[293]*See supra* notes 225 - 229 and accompanying text.

[294]*See supra* Part II(C)(1)(b).

[295]*See supra* Part II(C)(1)(b). *See also* LAFAVE, *supra* note 23, at § 5.5(C) ("conviction for strict-liability offenses should be insulated 'from the type of moral condemnation that is…implicit when a sentence of imprisonment may be imposed.'") (quoting MODEL PENAL CODE § 2.05, Comments (Tent. Draft No. 4, 1955).

liability.[296] We are not, after all, addressing conduct which is in any way analogous to a traditional "crime." The premise for imposing criminal liability upon "architects" is not that they have actively committed criminal acts, but that they have defaulted on a duty "not to act in such a way as to endanger the . . . general public."[297] If an "architect" were to intentionally incorporate a defect into software so it could be exploited by cyberterrorists or cybercriminals, we would use traditional principles of criminal law, i.e., complicity, conspiracy and substantive offenses, to hold him liable for what he had done. The rationale for imposing criminal product liability upon "architects" is functionally indistinguishable from the rationale used to craft other regulatory offenses;[298] the ultimate goal is to use a version of criminal liability to reinforce the duty to ensure that the products and/or services that are supplied do not harm the public directly or, in this instance, indirectly, by eroding the security of cyberspace.[299] Since criminal liability is being utilized for a regulatory purpose, the basic penalties imposed for criminal product liability offenses should be minor, most likely limited to fines.[300]

---

[296]*Cf.* Metzger, *supra* note 279, at 81 ("Prudence. . . seems to dictate that individual criminal liability for defective products be premised upon the defendant's reckless or knowing behavior which directly contributed to the proscribed harm").

[297]*See supra* note 291 and accompanying text.

[298]*But see infra* note 300.

[299]For yet another source of analogy, *see e.g.,* Kevin M. McDonald, *Don't Tread On Me: Faster Than A Tire Blowout, Congress Passes Wide- Sweeping Legislation That Treads On The Thirty-Five Year Old Motor Vehicle Safety Act*, 49 BUFF. L. REV. 1163, 1200 (2001) ("TREAD Act amends the Vehicle Safety Act to provide for criminal liability where a person violated reporting requirements . . . with respect to safety-related defects in motor vehicles or motor vehicle equipment").

[300]If we decide criminal product liability doctrines are more properly analogized to antitrust law than to the regulatory offenses discussed in the text above, then our approach should eliminate strict liability in favor of demonstrated culpability, presumably purposeful or knowing conduct, and should entail more severe penalties. As to culpability, we could employ a variant of the standard the Supreme Court set out in *United States v. United States Gypsum Co.*, 438 U.S. 422, 445-46 (1978):

(b) Civil Liability

The software industry' main arguments against subjecting it to civil product liability rests upon the assumption that adopting such liability would subject the industry to potentially hundreds of thousands of civil suits, a large percentage of which would be frivolous or would be seeking damages for de minimis injuries.[301] Further, it is assumed that dealing with all these civil suits would impose significant time, resource and incentive burdens on an industry that needs to be nimble, creative and focused if it is to design and supply the ever evolving tools needed to maximize the advantages that cyberspace offers to essentially every aspect of the human endeavor.[302] Critics of the software industry's arguments find these assumptions to be flawed. While they concede that extending civil product liability to software would produce "a

---

> The business behavior which is likely to give rise to criminal antitrust charges is conscious behavior . . . undertaken only after a full consideration of the desired results and a weighing of the costs, benefits, and risks. A requirement of proof not only of this knowledge of likely effects, but also of a conscious desire to bring them to fruition or to violate the law would seem . . . both unnecessarily cumulative and unduly burdensome. Where carefully planned and calculated conduct is being scrutinized in the context of a criminal prosecution, the perpetrator's knowledge of the anticipated consequences is a sufficient predicate for a finding of criminal intent.

As to penalties, *see e.g.,* Raymond Krauze & John Mulcahy, *Antitrust Violations,* 40 AM. CRIM. L. REV. 241, 280 (2003) ("corporations convicted of antitrust felonies may receive fines equal to the greater of twice the corporation's pecuniary gain or twice the victim's pecuniary loss" and "[i]ndividuals may be fined up to a maximum of $350,000, sentenced to up to three years in prison, or both").

[301] *See supra* Parts II(C)(2) & II(C)(2)(a).

[302] *See, e.g., Dollars and Lives: The Cost of Shoddy Software,* USA TODAY, *at* http://www.usatoday.com/tech/news/2003-04-28-software-bugs_x.htm, (April 28, 2003) (last visited October 21, 2004); Harris Miller, *Penalizing Vendors Brings Consequences,* NETWORK WORLD FUSION, *at* http://www.nwfusion.com/columnists/2002/0422faceoffno.html. (April 22, 2002) (last visited October 21, 2004). *See also supra* note 258 and accompanying text. The burdensome effects of such suits could be exacerbated if the various states (and nations) adopted varying legal standards governing product defects.

blizzard of lawsuits," [303] they argue that the eventual effect of this litigation would be to improve software, not to degrade it.[304]

Both sides of the debate demonstrate valid points. Software is an admittedly complex product, far more difficult to design, maintain and upgrade than the real-world items to which product liability has traditionally been applied.[305] Thus, software product liability suits would be expensive, time-consuming and burdensome for both parties,[306] and their impact on software quality would nevertheless remain uncertain.[307] Set against this uncertainty, however, is the demonstrable fact that the current strategy of relying on market forces does not ensure that software is minimally reliable, let alone sufficiently secure to protect the national infrastructure.[308] Clearly, some other approach is required.[309]

---

[303]Mann, *supra* note 257, at 33, 38.

[304]*See, e.g., id*. at 38 ("the lawsuits will . . . come. And when the costs of litigation go up enough, companies will be motivated to bulletproof their code").

[305]*See, e.g., id.* at 36.

[306]*See, e.g., id.* at 38 ("lawsuits would be highly technical, which means that plaintiffs would need to hire costly experts to build their cases"). *See also* Jody Armour & Watts S. Humphrey, *Software Product Liability*, SOFTWARE ENGINEERING INSTITUTE, *at* http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr13.93.pdf (August 1993) (last visited October 21, 2004). For many of the same reasons, civil tort suits have proven an ineffective device for enforcing environmental standards. *See, e.g.*, Clifford Rechtschaffen, *Deterrence vs. Cooperation and the Evolving Theory of Environmental Enforcement*, 71 S. Cal. L. Rev. 1181, 1197-98 (1998) ("Private lawsuits alleging environmental harm . . . are very difficult to win . . . The cases are lengthy and expensive, requiring a great deal of expert testimony").

[307]*See supra* notes 302 - 304 and accompanying text.

[308]*See, e.g.*, Greg Cooper, *ACM Fellow Profile: Eugene H. Spafford*, SOFTWARE ENGINEERS NOTES, *at* http://www.acm.org/sigsoft/SEN/spafford.html (last updated July 31, 2001) (last visited October 21, 2004) ("It's about cost. If you make software better, you may be slower to market. Even if your product is more reliable and more secure . . .you may go out of business while the makers of inferior products continue to prosper"). *See also* Mann, *supra* note 254, at 34 ("many software engineers believe that software quality is not improving . . . . it's getting worse. It's as if the cars Detroit produced in 2002 were less reliable than those built in 1982"). For the annual increases in reported software vulnerabilities, *see, e.g.*, CERT/CC STATISTICS 1988-2003, CARNEGIE MELLON SOFTWARE ENGINEERING INSTITUTE, *at* http://www.cert.org/stats/cert_stats.html#incidents (last updated

The judicious use of criminal product liability is such an approach, one that could resolve the issues that arise with regard either to relying on market forces or to implementing civil product liability. Unlike civil product liability suits, criminal product liability prosecutions are brought by the state, which limits the number of actions brought and tends to filter out frivolous suits.[310] Further, unlike market forces, criminal product liability can be employed to create incentives to provide reliable, technically adequate software (or, perhaps more accurately, to create disincentives for producing software that is unreliable and technically inadequate).[311]

While such criminal product liability has been analyzed above;[312] this discussion is concerned with how it should be enforced. Enforcement becomes an issue for criminal product

---

Aug. 3, 2004) (last visited October 21, 2004). *But see* Rich Mogull & Richard Hunter, *Cyberattacks and Cyberterrorism: What Private Business Must Know*, GARTNERG2, *at* http://www.gartnerg2.com/qa/qa-0902-0091.asp (September 25, 2002) (last visited October 21, 2004) ("Bush Administration . . . will rely on market forces to improve security" of software). For another area in which reliance on market forces has proven insufficient to induce compliance with a desired standard, see Rechtschaffen, *supra* note 306, at 1196.

[309]*See, e.g.*, Declan McCullagh, *A Legal Fix for Software Flaws?*, ZDNET, *at* http://zdnet.com.com/2100-1104_2-5067873.html (August 26, 2003) (last visited October 21, 2004)

> ([R]epeated failures are leading . . . security experts to press for changes in software liability law to better motivate companies to fix . . . insecure code. `If the laws . . . forced software makers to be held liable – criminally, civilly, financially – for their products, we'd see a marked increase in product quality, security and stability,' said Richard Forno, an author and security consultant).

[310]Prosecutions must be based on probable cause to believe a crime has been committed by the person being charged; this is a higher standard than that required for the initiation of civil suits and it serves to reduce, if not eliminate, baseless actions. *See, e.g.*, ABA STANDARDS FOR CRIMINAL JUSTICE, 3-3.9(a) (3d ed. 1993) ("A prosecutor should not institute . . . criminal charges when the prosecutor knows that the charges are not supported by probable cause"). *See generally* Gerstein v. Pugh, 420 U.S. 103, 112-114 (1975). The filtering effect resulting from the probable cause standard is enhanced by the fact that prosecutions are initiated by prosecutors who are trained in the law and, unlike civil litigants, have no personal stake in the initiation of a particular proceeding. *See, e.g.*, ABA STANDARDS FOR CRIMINAL JUSTICE, 3-3.9(d) ("In making the decision to prosecute, the prosecutor should give no weight to the personal or political advantages . . . which might be involved or to a desire to enhance his or her record of convictions").

[311]*See supra* Part II(C)(2)(a).

[312]*See supra* Part II(C)(2)(a).

liability because it is not a traditional use of criminal liability. Criminal liability has traditionally been used to sanction individuals who affirmatively inflict harm by committing crimes; the goal is to denounce and punish offenders whose behavior threatens internal order.[313] Since traditional miscreants actively and contumaciously engage in conduct that threatens the social order, the default assumption is that each of them (or as many as possible) should be apprehended, prosecuted and punished;[314] their conduct represents behavior which, to varying degrees, society simply will not tolerate.[315] The criminal product liability principles postulated here are not concerned with this type of traditional, active criminal behavior. The goal of a criminal product liability law would be to enforce a duty to supply reliable, technically adequate software by identifying and sanctioning those who fail to discharge this obligation.[316] The question then becomes: How *much* enforcement is appropriate? Should the traditional criminal law assumption that every offender should (ideally) be prosecuted and punished apply here?[317]

One could argue that given the gravity of the potential consequences of failing to discharge the duty to supply reliable, technically adequate software,[318] the default assumption of

---

[313]*See supra* Part I. *See, e.g.*, Sayre, *supra* note 280 at 68 ("… original objective of the criminal law was to keep the peace . . . . "); *see also* LAFAVE, *supra* note 23, §1.2(e).

[314]*See, e.g.*, AMERICAN BAR ASS'N STANDARDS FOR CRIMINAL JUSTICE 3-3.9 cmt. (3d ed. 1993) ("A prosecutor ordinarily should prosecute if, after full investigation, he or she finds that a crime has been committed, the perpetrator can be identified, and there is sufficient admissible evidence available to support a verdict of guilty.").

[315]*See supra* Part I. *See also* Goodman & Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, *supra*, 2002 UCLA J. L. & Tech. at 56.

[316]*See supra* Part II(C)(2)(a).

[317]The strategy is an ideal because, of course, "there are not enough enforcement agencies to investigate and prosecute every criminal act that occurs." AMERICAN BAR ASS'N STANDARDS FOR CRIMINAL JUSTICE 3-3.9 cmt. (3d ed. 1993).

[318]*See supra* Part II(C)(2)(a). Under certain circumstances, traditional criminal liability is imposed for not acting; *see, e.g.*, LAFAVE, *supra* note 23, § 6.2. Such liability is generally restricted to instances in which someone who had a legal duty to another failed to perform a relatively straightforward act which he or she was physically capable of

prosecuting every offender should apply. This assumes that the "harm" caused by criminal product liability offenses should dictate the enforcement strategy; but while that assumption holds for traditional criminal behavior,[319] there are compelling reasons why it should not apply to criminal product liability offenses. One is that unlike traditional criminal liability, criminal product liability is based on inaction; one is not held liable for actively sabotaging software, but for failing to ensure it is of acceptable quality.[320] Another reason is culpability. Traditional criminal liability is based on a truly "bad mind;"[321] that is, it requires a specific level of culpability (i.e. intention) relative to the course of conduct carried out by one or more persons, e.g., robbing a convenience store, stabbing another person, or executing a Ponzi scheme.[322] The defining characteristic of traditional criminal liability is the perpetrator's intention to cause some type of "harm."[323] The intent to cause "harm" makes traditional offenders "dangerous" and that accounts for the default enforcement strategy, i.e., that every offender should be apprehended

---

performing*; see id.* The relative simplicity of the conduct at issue differentiates this type of omission liability from criminal product liability.

[319]*See, e.g.*, AMERICAN BAR ASS'N STANDARDS FOR CRIMINAL JUSTICE 3-3.9(b)(ii) (3d ed. 1993).

[320]*See supra* Part II(C)(2)(a).

[321]*See, e.g.*, 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 21 (Professional Books Limited 1982) (1808). ("to constitute a crime against human laws, there must be, first, a vicious will . . .).

[322]A Ponzi scheme is a type of fraud in which investors are paid "exceptional dividends" based on funds deposited by new investors. Mark Fleming, *Bubble and Ponzi Schemes used in Investment Fraud Scams* (May 2002), http://www.crimes-of-persuasion.com/Crimes/InPerson/MajorPerson/ponzi.htm. As to culpability, *see, e.g.*, LAFAVE, *supra* note 23 at § 5.1; For the proposition that traditional criminal liability assumes relatively simple conduct and one or only a few offenders, *see, e.g.*, Brenner, *supra* note 69; Traditional criminal liability can be imposed on those who participate in complex real-world criminal activity, such as large-scale drug-dealing. *See, e.g., United States v. High*, 117 F.3d 464, 466-467 (11th Cir. 1997); But even in a complex drug operation involving many participants, the essential conduct is simple and straightforward -- i.e., procuring drugs, distributing drugs and taking care of related matters such as security -- compared to what is involved designing and manufacturing the software (and hardware) used to participate in cyberspace. *See supra* Part II(C)(2)(a).

[323]*See supra* note 321.

and sanctioned.[324] Criminal product liability, on the other hand, requires no culpability, and thus has a strict liability standard; it applies this standards to extraordinarily complex, collaborative activity carried out by hundreds or even thousands of individuals.[325] The complexity of this activity can undermine an individual's or an entity's ability to control the conduct at issue.[326] Producing reliable software is, after all, a far more complicated process than keeping rodents out of a Baltimore warehouse.[327]

The use of strict liability coupled with the complexity of the activity at issue requires a different enforcement strategy for criminal product liability, at least as it is applied to software. It would have to filter out cases when prosecution would be technically permissible but is inapposite for other reasons.[328] The enforcement strategy used for environmental crimes (which can also involve complex, collaborative activity) could be adapted for this purpose.

---

[324]*See, e.g.*, JEROME HALL, GENERAL PRINCIPLES OF CRIMINAL LAW 213-22 (2d ed. 1960)*; see also supra* note 317, 3-3.9 cmt.

[325]*See supra* notes 291 - 296 and accompanying text*; see generally* LAFAVE, *supra* note 23, §5.5.

[326]*See supra* note 325 and accompanying text*; see also supra* Part II(C)(2)(a)*; see, e.g.*, Mann, *supra* note 257 at 35 ("…coders make 100 to 150 errors in every thousand lines of code they write . . . "). Individual versus corporate liability is discussed at the end of this section.

[327]*See supra* Part II(C)(2)(a).

[328]As noted above, relying on criminal liability introduces an initial filtering mechanism: Fewer criminal than civil product liability cases would be filed because (a) prosecutions are brought by the state, not by discrete, aggrieved individuals and (b) each prosecution would be based on the infliction of a collective "harm." *See supra* Part II(C)(2)(a); This is consistent with the concept of regulatory, or "public welfare" offenses: The development of regulatory offenses was based in part on "on the notion that it was more convenient for the state to bring an action affecting a group of persons in a criminal proceeding rather than place the burden of proof of direct harm on certain individuals in a civil suit." Barber, *supra* note 280 at 112; The *Park* case, for example, involved one prosecution for the adulteration of the food in the Baltimore warehouse, not thousands of civil suits brought by individuals who were harmed by the adulterated food. *See supra* Part II(C)(2)(a).

The Environmental Protection Agency ("EPA") and the Department of Justice ("DOJ") cooperate in enforcing the criminal provisions of most federal environmental statutes.[329] The EPA investigates potential violations and can request prosecution in appropriate cases;[330] its policy is to seek criminal sanctions only if "both significant environmental harm and culpable conduct are present."[331] The EPA will not make a criminal referral to the DOJ if a violator in good faith identifies, discloses and corrects violations, unless they "(i) involve criminal acts of individual managers or employees; (ii) there exists a management philosophy condoning environmental violations; or (iii) there is conscious participation in, or willful blindness to, the violations by high-level corporate employees."[332] The DOJ has a similar policy that articulates factors federal prosecutors are to consider "in determining whether and how to prosecute" when "the law and evidence would otherwise be sufficient for prosecution."[333] Essentially, they are to consider "(i) voluntary disclosure [of violations]; (ii) the degree and timeliness of cooperation; (iii) preventive measures and compliance programs; (iv) pervasive non-compliance; (v) disciplinary systems to punish employees who violate compliance policies; and (vi) subsequent

[329]*See* Rachel Glickman, et al., *Environmental Crimes*, 40 AM. CRIM. L. REV. 413, 416 (2003)*; see also id.* at 427-428*; see, e.g.*, U.S. DEP'T OF JUSTICE, FACTORS IN DECISIONS ON CRIMINAL PROSECUTIONS FOR ENVIRONMENTAL VIOLATIONS IN THE CONTEXT OF SIGNIFICANT VOLUNTARY COMPLIANCE OR DISCLOSURE EFFORTS BY THE VIOLATOR § I (July 1, 1991), http://www.usdoj.gov/enrd/factors.htm (DOJ policy "to encourage self-auditing, self-policing and voluntary disclosure of environmental violations by . . . indicating that these activities are viewed as mitigating factors in the Department's exercise of criminal environmental enforcement discretion.").

[330]*See, e.g.*, Clean Air Act, 42 U.S.C. § 7413(a)(3)(B), (c) (2000).

[331]Glickman, et al., *supra* note 329 at 416; Levels of culpability in federal environmental statutes range from "knowingly" to negligently. *See, e.g., id.* at 445-46, 449.

[332]*Id.* at 428*; see also* David A. Barker, Note, *Environmental Crimes, Prosecutorial Discretion and the Civil/Criminal Line*, 88 VA. L. REV. 1387, 1406 (2003) ("From 1996 to 1998, EPA averaged just 269 referrals to DOJ for criminal prosecution, or about one criminal referral for every fifty administrative enforcement actions.").

[333]U.S. DEP'T OF JUSTICE, *supra* note 329 § II.

compliance efforts."[334] The overall goal is to encourage self-policing and voluntary compliance.[335]

The DOJ's policy of using criminal liability selectively while encouraging self-policing and voluntary compliance as ways to avoid prosecution is an effective approach to the enforcement of criminal laws that target sophisticated, complex activity which typically occurs in a corporate context. It combines deterrence- and compliance-based enforcement.[336] While the

> theoretical underpinning of the . . . system relies . . . on deterrence, in practice the process is much more flexible. Most enforcers use a hybrid strategy that includes elements of both coercion and cooperation. . . . Most enforcement . . . is aimed at bringing violators back into compliance rather than punishing or deterring. Most

[334]Glickman, et al., *supra* note 329 at 417*; see* U.S. DEP'T OF JUSTICE, *supra* note 326 § II.

[335]*See* Glickman, *supra* note 329, at 416. A similar process is used to initiate the type of criminal proceeding at issue in the *Park* case, discussed in Part II(C)(2)(a):

1. An inspection is conducted by an FDA investigator and a report is prepared.
2. Where inspection reveals violative conditions, the inspection report is referred to the Compliance Branch of the field office for review.
3. The field office may then recommend appropriate regulatory action … to the pertinent FDA Bureau.
4. Where the possible legal action is criminal prosecution, the field office provides potential defendants with an Opportunity to Present Views, pursuant to 21 U.S.C. § 335, and 21 CFR 7.84 *et seq* . . . The record from the hearing is then reviewed by the field office in determining appropriate legal action, if any.
5. The field [office's] recommended course of action is reviewed by the Bureau. If the Bureau concurs . . . the matter is then referred . . . to [the] Enforcement Policy Staff.
6. Recommendations for regulatory action, if approved by [that] office, are referred to the Office of General Counsel of FDA for review and approval.
7. If approved by FDA's Chief Counsel, then *and only then*, is a matter formally referred to Justice (through the appropriate U.S. Attorney) for the institution of legal proceedings.

United States v. Gel Spice Co., 773 F.2d 427, 428 (2d Cir. 1985)*; see* 733 F.2d at 428-432*; see also* U.S. Dept. of Justice, U.S. Attorneys' Manual § 4-8.010 (2002), *available at* http://www.usdoj.gov.usao/eousa/foia_reading_room/usam/title4/civ00104.htm, (last visited September 23, 2004).

[336]*See, e.g.*, Rechtschaffen, *supra* note 306, at 1186-90. For the ineffectiveness of a compliance-based enforcement, *see id.* at 1191-1201.

instances of noncompliance are met with either no sanctions or only minor, informal ones.[337]

A similar approach could be used to implement criminal product liability for software. The use of criminal liability combined with the internal review and filtering processes described above (i) resolves the "litigation overload" objections the software industry raises to civil product liability; (ii) resolves similar objections that would no doubt be raised to the implementation of an unfiltered criminal product liability; and (iii) fills the vacuum that results from relying on market forces to improve software.[338] The resolution of (ii) requires parsing enforcement authority out within jurisdictions; that is, it would be necessary to specify which entities were authorized to initiate criminal product liability proceedings at the state and federal levels.

Prosecution authority at the federal level would certainly reside with the DOJ. The authority to initiate criminal product liability prosecutions could be given to the Criminal Division of the DOJ[339] or to a special enforcement unit analogous to the Antitrust or Environmental and Natural Resources Divisions.[340] It would be necessary to decide whether local U.S. Attorney offices could also initiate such prosecutions; given the technical complexity of the issues and the need for consistency in such prosecutions, it seems advisable to reserve prosecution for the Criminal Division or for a special enforcement unit created for this

[337] *Id.* at 1189 (note omitted).

[338] *See supra* notes 305 – 309 and accompanying text.

[339] *See* U.S. Dept. of Justice, U.S. Attorneys' Manual tit. 9, *available at* http://wwwusdoj.gov/usao/eousa/foia_reading_room/usam/title9/title9.htm, (last visited September 23, 2004).

[340] *See* U.S. Dept. of Justice, U.S. Attorneys' Manual tit. 5 & 7, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title5/title5.htm, (last visited September 23, 2004); http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title7/title7.htm, (last visited September 23, 2004).

purpose.[341] A similar system should govern prosecution at the state level; that is, prosecutions should be handled by a central, specialized unit and not by local prosecutors. Allowing criminal product liability prosecutions to be initiated by local prosecutors would undermine the efficacy of the enforcement strategy outlined above.[342] For one thing, local enforcement would effectively eliminate the filtering process that can be achieved by reserving these cases for a special unit which encourages compliance and uses prosecution selectively.[343] It would also, without doubt, produce failed prosecutions, as local prosecutor offices generally do not have the resources needed to litigate such complex cases effectively.[344] Failed prosecutions would undermine the strategy outlined above by introducing elements of inconsistency into the enforcement process; and consistency in enforcement is essential for a strategy targeting activity that is national – indeed, international – in scope.[345] Therefore,

---

[341]Most antitrust prosecutions are handled by the DOJ's Antitrust Division; local U.S. Attorney's offices can initiate certain types of antitrust prosecutions, but they are subject to review by the Antitrust Division. *See* U.S. Dept. of Justice, U.S. Attorneys' Manual § 7-1.100 (1997), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title7/1mant.htm, (last visited September 23, 2004) (review "ensures a consistent national policy on antitrust questions"). Local U.S. Attorney's offices can initiate environmental prosecutions except in cases of "national interest." *See* U.S. Dept. of Justice, U.S. Attorneys' Manual § 7-1.100 (2001), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title5/11menv.htm#5-11.105, (last visited September 23, 2004)…and [the Environmental Crimes Section of the DOJ] will participate jointly as co-counsel from the initiation of the investigation through prosecution." *Id.*

[342]*See supra* notes 329 – 337 and accompanying text.

[343]*See id.* Selective prosecution, in this context, means that prosecutions are not brought automatically but are subject to a screening process analogous to that which the DOJ uses for environmental cases. *See supra* notes 329 – 337 and accompanying text.

[344]*See supra* note 306 and accompanying text. *See, e.g.*, Metzger, *supra* note 279, at 2 (Ford Motor company, which was prosecuted for manslaughter based on its distributing a dangerously defective vehicle, was acquitted).

[345]*See e.g., supra* note 341. *See also* National Association of Attorneys General, NAAG Projects: Antitrust: Multistate Task Force, *at* http://www.naag.org/issues/issue-antitrust-multi.php, (last visited September 23, 2004)

prosecution authority at the state level, as at the federal level, should be allocated to a centralized unit. One approach, which is consistent with practice in other areas, is to assign exclusive authority for bringing criminal product liability prosecutions against software manufacturers to a unit in the state Attorney General's office.[346]

We must address a final enforcement issue: Should prosecutions target the entity that distributes flawed software, the individuals whose actions proximately cause the flaws, or both?[347] The best approach is to allow prosecution for both; in the *Park* case, after all, the corporation and its president were prosecuted for allowing food to become adulterated.[348] The rationale for prosecuting offending entities is that it advances specific and general deterrence by encouraging the offenders, and similarly-situated entities, to institute policies to prevent the recurrence of such an event.[349] The rationale for prosecuting individual employees who are to

---

("For over twenty years, State Attorneys General have worked together to bring multistate cases to protect . . . consumers. These joint actions ensure consistent enforcement of state antitrust . . . laws).

[346]*See, e.g.*, ME. REV. STAT. ANN. tit. 35, §7106(5) (West Supp. 2003).

[347]The statement of this issue assumes, as it seems likely, that software design and manufacture will take place in an organizational context.

[348]*See supra* Part II(C)(2)(a).

[349]*See supra* note 23 and accompanying text. *See, e.g.*, Philip Urofsky, United States Department of Justice Memorandum Regarding Federal Prosecution of Business Organizations (January 20, 2003) in Practicing Law Institute, Corporate Law and Practice Course Handbook Series, PLI Order No. B0-01NM 813 (April-June, 2003) ("Although non-criminal alternatives to prosecution often exist, prosecutors may consider whether such sanctions would adequately deter . . . a corporation that has engaged in wrongful conduct"). *See also id.:*

> Non-criminal sanctions may not be an appropriate response to an egregious violation, a pattern of wrongdoing, or a history of non-criminal sanctions without proper remediation. . . . In determining whether federal criminal charges are appropriate, the prosecutor should consider the same factors . . . considered when determining whether to leave prosecution of a natural person to another jurisdiction or to seek non-criminal alternatives to prosecution. These factors include: the strength of the regulatory authority's interest; the regulatory authority's ability and willingness to

some degree personally responsible for an entity's defaulting on its duty to provide satisfactory software is that it reinforces the entity-deterrent effect by giving employees a "personal stake" in their employer's compliance with the law;[350] indeed, according to one view, holding individual employees liable can "provide the strongest deterrent against future corporate wrongdoing."[351] Authorizing prosecution for both does not mean, of course, that both should be prosecuted in every case; the decision to prosecute one, both or neither necessarily depends on the facts of each case, but a decision to prosecute an entity should not bar prosecution of employees.[352]

III. TOKUGAWA CYBERSPACE

. . . control without authority.[353]

To drastically oversimplify, there are two approaches to maintaining internal order in a human social system.[354] One approach is to rely on formally promulgated, objective rules –

---

take effective enforcement action; the probable sanction if the regulatory authority's enforcement action is upheld; and the effect of a non-criminal disposition on Federal law enforcement interests.

This memorandum notes the need to consider specific and general deterrence in deciding whether to charge a corporation. *See id.* at 814.

[350]*See, e.g.,* David G. Dickman, *Recent Developments in the Criminal Enforcement of Maritime Environmental Laws*, 24 TUL. MAR. L.J. 1, 2 (1999) ("Whenever possible, federal and state law enforcement officials will… prosecute corporate officers and other individuals … because prosecution of individuals is viewed by the Department of Justice … as the strongest deterrent to environmental crime").

[351]Mary Jo White, Criminal Enforcement of the Securities Laws, Practising Law Institute, Corporate Law and Practice Course Handbook Series, PLI Order Number B0-01PG 1145 (November, 2003).

[352]*See, e.g.,* U.S. Dept. of Justice, U.S. Attorneys' Manual § 5-11.114 (2001), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title5/11menv.htm#5 -11.114, (last visited September 23, 2004) ("In any case against both a corporation and any of its individual employees the willingness of the offending corporation to enter a guilty plea is not a basis for dismissal as against the individual").

[353]*See supra* note 2 and accompanying text.

[354]*See supra* Part I.

"laws" – that are enforced by a specific social structure or institution;[355] this approach has been used for centuries in the Western world.[356] It relies upon legal codes to articulate the rules that govern conduct in a society and upon police, lawyers and courts to enforce these rules.[357] In such a social system, "law" is an external, hierarchically enforced constraint on behavior; it is an externality one ignores at the peril of suffering sanctions.[358] This is the system to which those of us raised and educated in Western cultures are accustomed, and it is the system we seek to impose upon the experiential reality known as cyberspace.

The other approach, practiced in parts of the historic Eastern world, relies on customary (i.e., not formally promulgated) rules that are embedded in the culture and enforced informally through one's relationships and interactions with others in the society.[359] This system prevailed

---

[355]*See, e.g.,* John Owen Haley, AUTHORITY WITHOUT POWER: LAW AND THE JAPANESE PARADOX 7 (1991) ("An institutionalized system is one in which . . . the making and enforcing of rules occur through established procedures and institutions – functions exercised by established political authority").

[356]*See, e.g.,* Dan Fenno Henderson, *Comparative Law in Perspective*, 1 PAC. RIM. L. & POL'Y J. 1, 5 (1992) ("Tokugawa . . . governance . . . did not involve official application of legal rules … as in Western adjudication. Westerners, from the Greeks and the Biblical era onward, have seen 'law' as based on principle – universal, given, and external to those bound").

[357]As explained earlier, this type of system also uses informal rules – norms – to structure much of a society's behavior in predictable, acceptable ways. *See supra* notes 171 – 176 and accompanying text. The behaviors controlled by norms tend to be behaviors that do not significantly intrude upon others' rights or interests; in legalistic systems, norms generally guide behavior into channels that promote social acceptance. In modern Western societies, for example, norms guide interactions with others so that we know, for instance, to go to the end of a queue instead of to the front or to defer to our boss, our teacher, our minister or others in a position of authority. In these systems, the consequences of violating informal rules tends to be limited to a loss of social acceptance which, while it can have detrimental personal and professional consequences, does not rise to the level of formal social sanctioning.

[358]*See supra* note 356. *See also supra* Part I.

[359]*See, e.g.,* HALEY, *supra* note 355, at 7 ("A…customary order…is one in which rules are either made or enforced or both by means of consensus and habitual community behavior."). *See also* Henderson, *supra* note 356, at 4 (Western societies depend "on a legal system and courts" for "dispute resolution and for maintenance of order in society" but "China had no such things in its culture as law, courts or adjudication").

in Japan, notably during the Tokugawa era, until Westerners rather insistently introduced their formal, legalistic approach to maintaining order in society.[360] This system does not require a formal institutional structure to enforce a set of external "laws;" instead of being an external, hierarchically enforced constraint on behavior, the rules that sustain internal order are part of the fabric of everyday life.

To understand how this system – which is so very different from modern Western systems with their laws and law enforcers – works, it is helpful to consider Japan during the Tokugawa period.[361] "In 1603, after generations of turmoil Tokugawa Ieyasu was appointed

[360]*See infra* note 361. Japan's system, like that of China, relied on Confucianism as the philosophical basis for maintaining internal order. *See, e.g.*, Glenn R. Butterton, *Pirates, Dragons and U.S. Intellectual Property Rights in China: Problems and Prospects of Chinese Enforcement*, 38 ARIZ. L. REV. 1081, 1108-11 (1996). *See generally* HALEY, *supra* note 355, at 29-32; 55; 62-63. *See also* Dean J. Gibbons, *Law and the Group Ethos in Japan*, 3-FALL INT'L LEGAL PERSP. 98 (1990).

[361]*See, e.g.*, HALEY, *supra* note 355, at 51-65 ("The Tokugawa regime endured until the forcible opening of Japan by the West in the mid-nineteenth century."). *See also id.* at 67-80. Victor Koschmann uses the contrasting concepts of "hard rule" and "soft rule" to explain the dramatic differences between Tokugawa society and modern Western legal systems. He argues that the

> Western past – subjugation, conflict, and violence – engendered rule by force, or `hard rule.' In these conditions, looking around at conflicts and open brutality, the individual sees himself `as prior to social forms, as their creator.' The state becomes abstract and remote. This . . . supports the development of transcendent norms; when groups and individuals are frank about their interests and pursue them at the expense of others, they testify to the existence of a higher truth – principles that are constant in every setting. In Japan, . . . this open competition never flourished, and consequently authority could maintain an ideal of unity between citizen and ruler, a soft rejection of duality and individuation.

Anita Bernstein & Paul Fanning, *"Weightier Than a Mountain": Duty, Hierarchy, and the Consumer in Japan*, 29 VAND. J. TRANSNAT'L L. 45, 62-63 (1996) (*quoting* J. Victor Koschmann, *Introduction: Soft Rule and Expressive Protest*, *in* AUTHORITY AND THE INDIVIDUAL IN JAPAN: CITIZEN PROTEST IN HISTORICAL PERSPECTIVE, 1, 18-19 (J. Victor Koschmann ed. 1978).

Shogun" and for "nearly three centuries Japan enjoyed . . . political peace and social stability."[362] The "pivotal element of the Tokugawa legal order" was the village, or *mura*;[363] a *mura* was one of the three basic administrative units of the Tokugawa system.[364] The *mura* was essential to maintaining internal order because by the end of the eighteenth century, Japan had a population of about 26.5 million but the Tokugawa regime had only forty *daikan*, or deputies, to implement its edicts.[365] While the Tokugawa shogunate issued edicts directed at the villages, it could not enforce them. Control over behavior therefore fell to the local administrative unit, which for most people was the *mura.*[366]

For all intents and purposes, a *mura* was an autonomous entity. However, to remain autonomous it had to maintain order: "So long as peace prevailed . . . there was little to draw official attention. . . . [A]ny open conflict or breach of peace threatened that autonomy and invited . . . more stringent controls."[367] A *mura* was a tightly-knit social, economic and political

[362]Gibbons, *supra* note 360, at 100. "Prior to Tokugawa rule, civil war continued intermittently from the 12th Century to the…17th Century." *Id.* at 100 n.6. For the unrest in the earlier period, *see, e.g.*, HALEY, *supra* note 355, at 58.

[363]HALEY, *supra* note 355, at 58.

[364]*Id.* at 58-59. The three basic units were the province, the district and the village. *Id.* at 58.

[365]*Id.* The *daikan* were responsible for overseeing activity outside Edo, where the shogunate was located. *Id.* at 55. As such, they were "the only official link between the . . . shogunate . . . and the vast majority of Japanese who resided in rural villages." *Id.* at 55-56.

[366]*Id.* at 60. *See also* MIKISO HANE, PREMODERN JAPAN: A HISTORICAL SURVEY 148 (1991). The essential irrelevance of shogunate regulation is demonstrated by the fact that the "Tokugawa tradition held that knowledge about the law was an elite preserve; even the criminal law was unpublished, and statesmen kept the correspondence between offenses and penalties secret." Bernstein & Fanning, *supra* note 361, at 64 (*quoting* HIDEO TANAKA, THE JAPANESE LEGAL SYSTEM: INTRODUCTORY CASES AND MATERIALS 164 (1976)).

[367] HALEY, *supra* note 355, at 61.

entity in which survival depended upon villagers' cooperating with one another.[368] Tokugawa villages consequently used social cohesion to maintain internal order,[369] with a villager's primary goal being to maintain harmony in his or her community.[370] Like other social systems, Tokugawa villages used rules to structure behavior and reduce conflict;[371] *mura* rules were parochial, informal and pragmatic, designed to maintain life as it had existed for centuries.[372] They were enforced by the villagers, who imposed sanctions for rule violations. The most common sanction was "community displeasure," but the Tokugawa villages also used "more severe forms of community coercion, such as ostracism and expulsion."[373]

Life in Tokugawa Japan is relevant to this article because the first step in developing a truly new approach to security in cyberspace is understanding how we conceptualize our

---

[368]*See, e.g.*, HITOMI TONOMURA, COMMUNITY AND COMMERCE IN LATE MEDIEVAL JAPAN: THE CORPORATE VILLAGES OF TOKUCHIN-HO 184 (1992). (Survival depended on exchanging labor "or the sharing of common resources, such as water for irrigation or forestland for fertilizer and building materials").

[369]*See, e.g.*, HALEY, *supra* note 355, at 61 ("[C]ommunity sanctions . . . were the real deterrents to wrongdoing in Tokugawa Japan.").

[370]*See, e.g.*, Jeffrey N. Lavine, *Foreign Investment in Japan: Understanding the Japanese System and its Legal and Cultural Barriers to Entry*, 9 B.U. INT'L L.J. 149, 151 (1991). The emphasis on harmony in Tokugawa Japan derived from Confucianism, which emphasized that the "proper role of the individual was to establish and maintain harmonious relationships rather than assert individual interests." Gibbons, *supra* note 360, at 103-04. *See generally supra* note 360. Indeed, in Tokugawa Japan, there was no conception of "law" in the Western sense. *See, e.g.*, Henderson, *supra* note 356, at 5. (In Tokugawa Japan, there was nothing "comparable to our ideas, concepts and institutions of 'law.'").

[371] *See, e.g.*, HALEY, *supra* note 355, at 62. *Mura* rule were not formally adopted nor were they regarded as "law." Tokugawa Japan did not differentiate between "law" and "morality," or ethics. *See, e.g.*, Christopher A. Ford, *The Indigenization of Constitutionalism in the Japanese Experience*, 28 CASE W. RES. J. INT'L L. 3, 14 (1996).

[372]*See, e.g.*, HANE, *supra* note 366, at 141-42:

> There was a village code that dealt with such basic concerns . . . as taxation, agriculture, and community activities. Those who violated the code of conduct . . . that regulated village affairs and the relationship between villagers were punished by the community. The punishments included . . . apologies, fines, ostracism, and banishment . . . .

[373]HALEY, *supra* note 355, at 61. *See, e.g.*, TONOMURA, *supra* note 368, at 184-85. *See also supra* note 372.

participation "in" cyberspace. We participate in cyberspace as individuals; we each "go it alone" when we are surfing the web or are otherwise engaging in online experiences. Much of the attraction of cyberspace is that it *is* a solitary, individual pursuit. "Individual pursuit" does not mean we do not engage or interact with others when we are online. It means we venture "into" cyberspace alone and unaccompanied; we structure our own experiences, we choose what we will or will not do, and we decide for how long we will do it.[374] Being "on our own" and unobserved, we do things – not necessarily criminal things – that we would probably never do "in public" out in the real-world. We can indulge our imagination and we can explore interests that may not be shared by anyone within hundreds or thousands of miles of our physical location. We can interact with others from far away, and in doing so, we can be no one (anonymous) or we can be someone else (pseudonymous). This freedom from the constraints we deal with in the real-world is an essential aspect of the experience; it is part of the attraction of cyberspace.

This model, a conceptualization of our participation in cyberspace, is an extrapolation of the way we experience real-space. In modern Western cultures, our participation in real-space tends to be atomized. We enjoy emotional (and financial) support from family and friends, but each of us is primarily responsible for structuring and implementing our participation in the real-world. We are responsible for successfully completing some level of education; for getting, keeping and discharging the obligations of employment; for securing transportation to and from work, school, recreation, etc.; for securing and maintaining housing; and for securing such basic necessities as food, clothing, and medical care. Ultimately, we are responsible for the various

[374]Families, for example, do not go "into" cyberspace together; family members go "into" cyberspace to engage in the respective activities each finds enjoyable. Venturing "into" cyberspace is an individual, not a shared, experience.

aspects of our personal lives (relationships, family, interests, etc.). The support we receive from others helps us in discharging these responsibilities, but we are ultimately and inevitably responsible for the success or failure of our various efforts.

This "individual" model of real-world experience is the evolved product of Western history. Over the last several centuries, Western societies have moved away from systems in which the family or community was responsible for structuring human endeavor to one in which responsibility is placed on the individual.[375] This shift is an unavoidable consequence of evolving from a rural, primarily agrarian society into an urbanized, mobile, technological society. In the former, people live their lives in stable collectives and stable environments (barring manmade or other disasters); one's life experience is routine, predictable and generally unproblematic, structured by an inherited fabric of customary rules and relationships. In the latter, people participate in life through a series of collectives, few of which are stable; even if one remains in the same job for years, he/she will almost certainly work with many different people as projects come and go and/or as other employees leave and new ones are hired. The same is true of contemporary, Western-style family and "community" life: People marry, have children, divorce, marry again, have children again, and perhaps divorce again. As a result, one's "immediate" and extended family becomes a series of shifting collectives. The concept of a localized community that shapes one's preferences and behaviors has little or no meaning for most people in contemporary Western-style societies. While there is a generalized, pervasive culture in these societies, it is far from homogeneous; it tends to be much more superficial in

[375]In Tokugawa Japan, for example, "individuals" did not exist – the "smallest legal unit was the family". Gibbons, *supra* note 360, at 101-02 n.11. A similar, though perhaps not quite so pronounced, emphasis on family and community was for centuries an essential element of Western cultures.

content and in effect than the stable, consistent culture found in more traditional societies.[376] Instead of engaging in behaviors and life patterns that are structured for us by family or community, we make our own choices and bear responsibility for those choices. By not having lives shaped and circumscribed by family or community, we rely more on formal rules and institutional rule-enforcers to sustain internal order. Laws and sanctions, instead of customary rules and "community displeasure," are used to define acceptable behaviors and discourage deviance.[377]

This adventitious model suits life in the contemporary, Western-influenced real-world. It is consistent with our ingrained assumptions about individual rights and responsibilities and the demarcation of authority between our individual selves and the agencies of the nation-state. We take no responsibility for ensuring internal order, aside from controlling our own behavior or taking minor actions such as installing alarm systems to discourage assaults on our safety and

[376]One has only to consider the complexity of the GRAMMY Awards, *GRAMMY Awards Process: Frequently Asked Questions*, GRAMMY.com, *at* http://www.grammy.com/awards/grammy/process.aspx (last visited Sept. 28, 2004) ("The GRAMMY Awards have 28 fields…and 105 categories within those fields."), or the amazing variety of publications available on Amazon.com to appreciate this. Amazon.com, *at* http://www.amazon.com/exec/obidos/tg/browse/-/283155/103-3834352-0389454 (last visited Sept. 28, 2004).

[377]*See, e.g.*, DONALD BLACK, THE SOCIAL STRUCTURE OF RIGHT AND WRONG 10 (rev.ed. 1998) ("Homogeneity…retards the use of law…"). A good example of this is the reaction to the baring of Janet Jackson's breast during the halftime show at the 2004 Super Bowl. The incident produced an outpouring of outrage on the part of Americans, most of which took the form of complaints to the Federal Communications Commission and other calls for "official" action to prevent further such incidents of broadcast "indecency." *See, e.g.,* Jonathan D. Salant, *Lawmakers Cite Super Bowl Halftime Show in Demands to Stop Indecency*, SAN DIEGO UNION-TIMES, February 11, 2004, http://www.signonsandiego.com/news/nation/20040211-1546-indecentprogramming.html, (last visited Sept. 29, 2004). *See also* Reuters, *Congress Focuses on Television Indecency: Fallout from Super Bowl Halftime Show*, CNN.com, February 11, 2004, *at* http://www.cnn.com/2004/ALLPOLITICS/02/11/house.decency.reut/index.html, (last visited Sept. 28, 2004). As explained earlier, we also rely on the internalization of informal rules – norms – to sustain internal order. *See supra* note 357. Indeed, it is internalizing a variety of informal rules that equips us to "take care of ourselves" out there in the real-world.

property. Unlike the villagers in a Tokugawa *mura*, we have divorced ourselves from the "policing" function, i.e., from the process of maintaining order in our collectivity. This is inevitable in complex, Westernized societies where the repertoire of behavior is far more convoluted and gradated than in rural, homogeneous societies like Tokugawa Japan.

This real-world model may not, however, be the appropriate default conceptualization for cyberspace. That does not mean that we should not experience cyberspace individually; on the contrary, individualism in cyberspace is an essential aspect of this quintessentially experiential reality. Nevertheless, it is already apparent that the devices we require in the real-world to maintain the baseline of internal order are not effective in cyberspace; and it is reasonable to assume that they will become increasingly ineffective as technology, and the experiential reality it sustains, become ever more sophisticated. Since the reactive model is not effective, we must find a new model; one founded on prevention is the only viable alternative.[378] The rules outlined in Part II(C) are designed to incorporate preventative components into the reactive model by holding "users" and "architects" liable, to different degrees and for different reasons, for failing to prevent cybercrime.

The problem relevant to "users" is that these rules are highly demanding, provided we are operating under our current conceptualization of cyberspace. "Users" are made responsible for securing their experience in cyberspace and the online experience of those for whom they are held responsible.[379] The goal is to alter assumptions and expectations and thereby create a climate of prevention; this requires a move from a reactive to a proactive strategy. The "user" rules outlined above are intended to initiate this process, [380] and they will undoubtedly have an

[378] *See supra* Part II(A)-(B).

[379] *See supra* Part II(C)(1).

[380] *See supra* Part II(C)(1).

impact on "user" behavior. Nonetheless, since their concern is with modifying individual behavior, the "user" rules fail to address another essential component of a preventative strategy. Currently, the greatest obstacle to achieving prevention and security at the "user" level is the difficulty of securing systems; and the difficulty of securing systems is a function of the complexity and the evolving nature of computer technology.

We need only to compare real-world and cyber-world security to understand why this is true. Burglar alarm technology is simple and quite stable. I can have a home security alarm system installed and can easily learn how to use it, at least until I need to learn a new system because the old one failed or because I move.[381] Computer technology, on the other hand, is neither simple nor stable. The laptop I recently purchased has anti-virus and other security software installed on it, but the software was out of date when I got it; indeed, it was probably out of date when my laptop left the manufacturer. Since I cannot rely on this technology, it is now up to me to update the software and to do whatever else is necessary to secure my online activities and prevent my becoming the victim of and/or a conduit for cybercrime.[382] This, however, is no easy task. The ever-evolving nature of computer technology coupled with the ingenuity of those who populate the "dark side" of cyberspace mean that anyone who goes online is effectively engaged in an "arms race" with cybercriminals (and cyberterrorists).[383]

---

[381]*See, e.g.*, Tom Davidson, Lorna Gentry & Steve McVey, *The Complete Idiot's Guide to Home Security* 159-159 (2001).

[382]*See supra* Part II(C).

[383]*See e.g., Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing, Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the S. Comm. on the Judiciary*, 106th Cong. (2000) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), http://www.mipt.org/pdf/cyberattacks03282001.pdf, (last visited September 27, 2003) (battle against cybercrime involves the "cyber equivalent of an arms race"). *See also* Jeanne Sahadi, *Cybercrime: Living With It,* CNN Money, Feb. 27, 2003, at

Computer security professionals and law enforcement officers find it difficult to compete successfully in this "arms race." How can we expect "users," who tend to be self-taught amateurs, to anticipate and withstand assaults from sophisticated attackers?[384]

This brings us to the possibility of re-conceptualizing how we participate in cyberspace. We could create "licenses" and otherwise regulate participation in cyberspace, and perhaps even limit it to those who are able to demonstrate that they possess the expertise and ability to fend off cyberattackers.[385] This approach is analogous to the way we have dealt with motor vehicles, the operation of which is also fraught with substantial perils.[386] For the cyber-world, however, this approach is neither desirable nor one that is likely to prove workable. Its undesirability lies in its

---

http://money.cnn.com/2003/02/20/commentary/everyday/sahadi/, (last visited September 27, 2004) (competition between online criminals and those responsible for computer security is an "arms race").

[384]*See, e.g.,* Joris Evers, *Security Suit Against Microsoft Could Turn Huge*, Info World, October 2, 2003, at http://www.infoworld.com/article/03/10/02/HNmssecsuit_1.html?security, (last visited September 27, 2004) (victim of identity theft suing Microsoft claims "Microsoft makes it too hard for consumers . . . to secure their systems").

[385]*See, e.g.,* Anick Jesdanun, *Digitally Informed: Should A License Be Required to Go Online?*, Detroit News, September 12, 2003, at http://www.detnews.com/2003/technology/0309/14/technology-268979.htm, (last visited September 27, 2004):

> Barely a day goes by without someone, somewhere getting stung or stinging others through careless Internet use.
>
> Though many of these threats are preventable, relatively few of us take the necessary precautions.
>
> So why not institute mandatory education before people can go online? After all, motorists must obtain licenses before they can legally hit the road, and computers are much more complicated. . . .
>
> Minimum competency requirements could include . . . how to update anti-virus programs, install firewalls and obtain security fixes for your computer's operating system . . . .
>
> Users . . . could become smarter about creating passwords and more cautious about using them at public terminals, where criminals have been known to harvest them with keystroke-logging software. . . .
>
> Dan Updegrove . . . is considering even more onerous requirements.
>
> `A car has to pass an inspection, and a driver has to pass a test,' he said. 'We need to be moving in the direction that machines are certified in some ways and users are certified in some ways.'

[386]*Id.*

overbreadth: It would, at least initially, deny the benefits and utilities of participating in cyberspace to a majority of the world's population as the price for markedly reducing the incidence of cybercrime.[387] It would transform cyberspace into an experience reserved for the techno-cognoscenti.[388] Reducing the incidence of cybercrime is certainly a desirable goal, but it is not worth this cost. We could markedly reduce the incidence of real-world crime by requiring everyone to wear government-issued identification badges, imposing curfews and otherwise restricting activity, but the costs, in terms of individual freedom and creativity, would far outweigh the benefits. A "licensing" approach would also be difficult to implement.[389] Who would issue the licenses? Who would monitor cyberspace to ensure only licensed participants were online? How often would licenses have to be renewed? Scofflaws pose another problem. I necessarily operate a motor vehicle in public, where I can be observed and can have my license checked; however, when I go online in private, it is far more difficult to detect my flouting of the law.[390] Thus, all the "licensing" approach would do is increase the burden on law enforcement by adding another layer of regulations and enforcement.[391]

Is there a way to preserve the "individual experience" of cyberspace while reducing the burden "users" currently labor under to secure that experience? One possibility is to introduce collectivities into the online experience. Instead of taking sole responsibility for protecting

---

[387] *See, e.g., id.* (A chief technology officer for computer security company noted that a "`downside is everybody you know won't be able to have a computer anymore, and I like being able to send e-mail to friends'").

[388] *See, e.g., id.* ("[W]hat do we do about the illiterate and the disabled, about people vexed by standardized tests? Bar them from the online world?").

[389] *See, e.g., id.* ("[W]ho's going to create and enforce the rules? A Federal Computing Commission or a United Nations for Computing?"). *See also id.* ("[T]echnology advances too quickly. Lessons become outdated. Repeat certifications would be necessary").

[390] *See supra* Part II(A)(4)(b).

[391] *See supra* Part II(A)(4)(b).

myself online, I could join with others in a collective – a twenty-first century version of a *mura* – the function of which would be to provide mutual support and thereby enhance the security of our online activities. Historically, when humans confronted disorder, they resorted to the premise that there is safety in numbers;[392] for the real-world, this denotes the combined physical force a group can muster to fend off attacks.[393] This has often meant meeting force with force; as noted earlier, however, strike-back techniques are not a desirable way to maintain order in cyberspace.[394] For the online world, the premise that safety lies in numbers should be construed as denoting a collective's ability to provide expertise, resources, moral support and the motivation to prevent and withstand attacks. Medieval Europe, for example, responded to attacks from Vikings and other outliers with a wave of urbanization.[395] Populations organized

---

[392]*See, e.g.*, NORMAN DAVIES, THE ISLES: A HISTORY 711, 963 (1999); ORLANDO FIGES, A PEOPLE'S TRAGEDY: THE RUSSIAN REVOLUTION 1891-1924 395, 644 (1998); WAR AND SOCIETY IN THE GREEK WORLD 92 (John Rich & Graham Shipley eds. 1995) (1993).

[393]*See, e.g.*, Azar Gat, *Why City-States Existed: Riddles and Clues of Urbanization and Fortifications, in* A COMPARATIVE STUDY OF SIX CITY-STATE CULTURES 125-38 (M. Hansen, ed. 2002), at http://cniss.wustl.edu/workshoppapers/gatpres2a.pdf (last visited September 27, 2004):

> [B]y coalescing around a central stronghold, people . . . ceased to present small, isolated, and highly vulnerable targets for raiders. . . . [T]here was increased safety in numbers . . . .[C]ities-towns were protected by *size*. Substantial settlements could not be quickly eliminated in a surprise night raid. Their inhabitants . . . comprised a considerable force and would have had time to wake up and resist. . . . [T]aking on a city meant direct fighting of the most severe, sustained, and dangerous sort: from house to house, with every building top potentially serving as a minor stronghold.

See also Urs A. Cipolat & Noah B. Novogrodsky, *Safety in Numbers: Bush Needs A Global Approach to Homeland Security*, Cal Law, January 23, 2002, at http://www.law.com/regionals/ca/opinions/stories/edt0123_cipolat.shtml (last visited September 27, 2004).

[394]*See supra* Part II(A)(4).

[395]DAVID NICHOLAS, THE GROWTH OF THE MEDIEVAL CITY: FROM LATE ANTIQUITY TO THE EARLY FOURTEENTH CENTURY 58-63 (Robert Tittler ed., 1997) ([U]rbanization increased in tenth century England because the "fortified centers offered more chance of survival…. Virtually all major English cities originated as fortifications that later

into collectives protected by walls and other fortifications were much more challenging targets than isolated farms or manors.[396]

The notion of importing collectivity into the online experience should not be interpreted as abandoning individuality or embarking upon some forced cyber-collective-farm experiment. It is simply a way to bring the essence of Tokugawa Japan's distributed, communal approach to maintaining internal order into the cyber-world. The purpose is to provide an alternative for those who do not feel they can protect themselves online; these "users" can participate in cyberspace via a collective that provides them with enhanced protection and mutual support.

How should this collective-participation alternative be implemented? It must, first of all, be an option; collective participation cannot be mandatory. Those who feel quite capable of protecting themselves online should not be forced into this option; all else aside, forcing competent "users" into collectives is inconsistent with our philosophy of individualism.[397] Since the strategy is to be purely voluntary, implementation should focus on encouraging those who are insecure about their ability to protect themselves online to participate in cyberspace via

---

developed commercial functions."). For a discussion of urbanization in other medieval European countries, *see id.* at 64-84. *See generally* Part II(B).

[396]*See supra* note 393. *See generally* JOHANNES BRONDSTED, THE VIKINGS 32-341 (1965); THE ANGLO-SAXON CHRONICLE 55, 70-72 (Trans. G.N. Garmonsway 1986) (1953).

[397]It would also require adopting and implementing a set of "do" rules which, as was explained earlier, is inadvisable in and of itself. *See supra* Part II(A)(4). The consequences of proceeding on one's own and falling prey to cybercriminals should help to encourage all but the most sophisticated "users" (along, no doubt, with those who perceive themselves as sophisticated "users") to take advantage of the relative security provided by collective access. *See supra* Part II(C)(1). Prosecutions of those who heedlessly eschew the collective alternative to become not only victims, but vectors for the victimization of others can reinforce the advisability of collective access for all but the most adept "users." *See supra* Part II(C)(1).

portals offering secure access.[398] American Online ("AOL") anticipates, to some extent, what such a portal might be like. AOL's stated goal is to provide a "safe and secure environment" for its subscribers;[399] to that end, it offers "powerful security safeguards,"[400] parental controls and other "family-focused solutions" to shield children from unfiltered Internet content[401] and to provide a "cash card" which teenagers can use for online purchases under their parents' supervision.[402]

The critical difference between a contemporary access service like AOL and the secure access portals being hypothesized here is that secure access is only a small part of what AOL offers its subscribers.[403] Secure access would be the defining characteristic of the collective access portals envisioned here; some portals might, as is explained below, also offer other services to their subscribers, but their universal *raison d'etre* would be security. These portals would be in the business of providing security online, just as companies like Pinkerton's or

---

[398]We already have web portals, in the form of websites that provide links to other sites. *See e.g.*, "portal," NetLingo, http://www.netlingo.com/lookup.cfm?term=portal (last visited September 27, 2004) (portal is a "web site that serves as a starting point to other destinations or activities on the web").

[399]*See e.g.*, AOL.com, Privacy Policy, *available at* http://www.aol.com/info/privacy.adp; AOL City Guide: Privacy Policy, AOL.com, *available at* http://www.digitalcity.com/aboutus/privacy.adp?change_city=1(last visited September 30, 2004).

[400]*See* Why Choose AOL?, Powerful Security Safeguards, *available at* http://www.aol.com/ why_choose_aol.adp. *See also* Optimized Security, AOL.com, http://www.aol.com/optimized/security.adp (last visited September 30, 2004).

[401]*See* AOL.com, Optimized for Families, *available at* http://www.aol.com/optimized/family.adp (last visited September 30, 2004).

[402]*See id.*

[403]AOL, for example, gives seven reasons why someone should choose AOL: (1) security; (2) a "family-friendly" environment; (3) enhanced communication; (4) a seamless experience with fast, reliable connections; (5) an "optimized broadband" experience; (6) "exclusive and on-demand programming"; and (7) "24/7 member services." AOL.com, Why Chose AOL?, *available at* http://www.aol.com/ why_choose_aol.adp (last visited September 30, 2004).

Brink's have traditionally provided security in the real-world.[404] This brings up yet another difference between these hypothesized portals and contemporary services like AOL: While AOL (and other Internet service providers) market themselves as providing security to their subscribers, what this really means is that they take responsibility for securing their own systems but leave subscribers responsible for protecting themselves online. AOL (and many other Internet service providers) do support subscribers' efforts in this regard by making available – either as part of the basic subscription service or as options that can be purchased separately – security devices ("tools") such as firewalls and antivirus software.[405] It is up to the individual subscriber to learn how to use these tools and to deploy them to protect himself when he is online. The portals hypothesized here, on the other hand, would guarantee their subscribers some level of secure online access that could (and no doubt should) extend to alerts about social engineering and other non-technologically based threats.[406]

While secure access portals styled after AOL would no doubt be an attractive choice for many "users," they could not be the only option; they would be perceived as too restrictive and too "safe" by many, and would consequently not be seen as an acceptable means of accessing

[404]See, e.g. Securitas Security Services USA, Inc., *available at* http://www.pinkertons.com/ (last visited September 30, 2004) (noting that Securitas, which is in the business of "protecting homes, work places and community", acquired Pinkerton's in 1999); The Brink's Company, *available at* http:/brinkscompany.com/ (last visited September 30, 2004) (noting that Brink's is "focused on protecting people and property").

[405]AOL, for example, provides "e-mail anti-virus protection," a firewall, pop-up blockers and a spam filter; subscribers can also purchase a "premium service" which supplies McAfee VirusScan Online. *See* Optimized Security, *available at* http://www.aol.com/optimized/security.adp (last visited September 30, 2004). EarthLink provides a similar set of alternatives, though its firewall must be purchased separately. *See* EarthLink Tools, *available at* http://www.earthlink.net/home/tools/ (last visited September 30, 2004); EarthLink Extras, *available at* http://store.earthlink.net/cgibin/wsisa.dll/store/main.html?type=extras (last visited September 30, 2004).

[406]*See, e.g.*, KEVIN D. MITNICK ET AL., THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 3-12 (2002).

cyberspace.[407] The best approach would be to have an array of portals that vary in the level of protection they provide and in the "culture" they offer. As to the former, portals could, as is explained below, offer different levels of secure access (correlating with different subscription costs); to encourage "users" to patronize portals, subscribing to portals with the highest levels of security could relieve them of criminal liability under the rules enunciated in Part II(C)(1).

AOL-style clones would offer not only access secure enough to negate potential criminal liability, but also a sanitized online experience; these portals would truly be gated communities, analogues of the current AOL system with its emphasis on filtered, host-generated content and experiences. Like AOL, these portals would presumably be attractive to families; they might also attract elderly "users" or other "users" who find unfiltered online content offensive because of their cultural or religious values or simply want to avoid unfiltered cyberspace. The portals might also offer some, though likely restricted, access to the "outside" world of cyberspace.

Another type of portal would only offer varying degrees of secure access. Like the AOL clones, some of the portals in this category would offer access that is secure enough to avoid the possibility of criminal liability for their subscribers; but unlike the AOL clones, these portals

---

[407] *See, e.g.*, Why *Greek Hate AOL*, THE GUARDIAN, Jan. 12, 2000, http://www.guardian.co.uk/efinance/article/0,2763,195777,00.html (last visited September 30, 2004):

> [N]etties don't like AOL. Search for `aol sucks' on the internet, and you'll find more than 4,000 web pages. But why? AOL is the world's most successful online service . . . .[O]n many hate lists the company rates up there alongside Microsoft and the government. All three are feared for the same reason: netizens worry that they are out to curb the . . . freedom of the internet, freedom to say things and choose particular technology to get around - or even dictate how they get online in the first place. . . .

See also Why AOL Sucks, *available at* http://www.ebtx.com/business/aolsucks.htm (last visited September 30, 2004) ("I've been trying to find a one word adjective that best fits AOL. The best I can come up with at present is *"cloying*"); Another AOL Sucks Commercial, *available at* http://www.jillsjokeline.com/aolsucks2.html (last visited September 30, 2004) ("American Online: The Choice of morons . . . everywhere").

would leave their subscribers free to enjoy an unfiltered online experience. Still other portals in this category could offer less secure access, on the premise that those ostensibly more sophisticated "users" would be attracted by the lower subscription costs and the cachet associated with assuming a risk of victimization and criminal liability. Finally, those confident in their own ability to "take care of themselves" online would be free to ignore the portals and access cyberspace on their own.

A level of secure access would be common to all portals; secure access is, after all, the primary reason for patronizing a portal. Portals could differ in other respects, though, including the basis upon which they were made available. The paragraphs above assume portals are commercial services: future analogues of AOL, EarthLink or other Internet Service Providers, all of which offer certain services in return for subscription fees. Many, if not most, portals would no doubt be commercial operations; subscription fees would be priced according to the level of secure access provided and whether a portal offered additional services, such as filtered online experiences. There could also be non-commercial portals. For example, companies could host portals as a new type of benefit, requiring employees to pay a fee for using their employer's secure systems to go online. Portals could be provided by colleges and universities (most of which already provide similar services for their students), by churches and by other organizations. Portals could be established by groups of like-minded people who choose to join together to establish a secure point of access; this access point could become a focal point of their activities and an emblem of their collective interests and identity.

In a sense, this concept of portals represents the implementation of a real-world strategy in the cyber-world. If we analogize cyberspace to a frontier territory in the real-world, the portals become outposts where people come together for security. They become, as noted above,

an online manifestation of the premise that there is strength in numbers; when faced with threats, they find it advisable to join with others to confront the danger.

This strength in numbers aspect of the portals would certainly contribute to their attractiveness to "users" and would be key in enhancing the security of cyberspace. There would, however, be another aspect of portals like those hypothesized above: They can help to alter expectations and assumptions and to create a climate in which "users" take some level of responsibility for online security. This last statement may seem contradictory, given that the primary purpose of portals is to relieve their patrons of at least some measure of responsibility for protecting themselves online. However, online threats are not constant; they evolve as technology and the resources, ingenuity and expertise of online criminals evolve. An important aspect of portals, therefore, is fostering a climate in which "users," at least those who do not limit their online activities to AOL-derived gated communities, are concerned about and are aware of new threats. The goal is to foster a sense of community which compels me to take responsibility for alerting the members of my community (e.g., the staff of the portal I patronize and its other subscribers) to any dangers I observe. Communication among community members regarding potential risks is not only an effective means of identifying such risks, but is also a means of reinforcing the need to be aware of them, to report any dangers one encounters, and to help other members of one's community become aware of risks that exist online and avoid them.[408] However effective portals of the type hypothesized above may become, risks will

[408]Portal members' communicating with each other about online dangers – including completed online victimization – will "personalize" cybercrime and bring home the need to avoid it. To understand why this is true, it is only necessary to consider a hypothetical: Assume that tonight, on ABC World News, I watch a story about a horrific homicide that takes place in Los Angeles, which is thousands of miles away from where I live. While I will be appalled at the crime and sympathetic to the victim and the victim's family, the crime will have no immediate significance to *me*; I do not see myself as running any conceivable risk of being victimized by the person who

always exist online, just as they will always exist in the real-world. In the online world, as in the real-world, the sense of commitment and moral support we derive from collective experience would prove to be an essential element in a strategy for preventing these dangers from being realized.[409]

IV. CONCLUSION

Tokugawa cyberspace will never really exist, but it is a useful metaphor for a new law enforcement strategy. As Part II explained, the reactive model of law enforcement we use to keep order in the real-world is not suitable for dealing with crime in the online world. This does not mean that we should discard that model; the concept of apprehending and sanctioning those who harm others should continue to be part of an online enforcement strategy, just as it will continue to be part of our real-world enforcement strategy. Nonetheless, it cannot be our sole, or even our primary, approach to cybercrime; the inherent impossibility of successfully reacting to

---

committed this crime. It becomes, therefore, a generalized threat, a reminder that dangers lurk even in the stable, safe real-world of the United States, but it not anything to which I need to take any particular cognizance. Now, assume that I see the same story but this time it is broadcast on a local news station in Dayton, Ohio, which is where I live; to make the hypothetical even more compelling, assume the murder was committed on the campus of the University where I teach. *Now* the homicide has "personal" significance – it has happened in a place I know, a place I frequent, and may even have happened to someone I know or know of. I now see this crime, the same crime at issue in the original version of this hypothetical, as something of which I need to take cognizance by taking certain precautions, changing my routine, buying Mace, etc.

One problem with raising "user" consciousness about cybercrime is that it tends to be perceived as a generalized threat, the online analogue of the Los Angeles homicide in the hypothetical presented above. Cybercrime "happens," but not to anyone I know; consequently, it has no personal significance for me. It is not a "real" threat. However, if information about cybercrime and reports of particular cybercrimes circulated through a portal such as that described above, the "fact" of cybercrime would be perceived as something "real," as something that could happen to me or to those whom I care about. Perceiving a threat as "real" is an essential first step in taking measures to avoid becoming the victim of such a threat.

[409] This aspect of the portals essentially provides an empirical predicate for the implementation of a variant of the community policing discussed earlier. *See supra* notes 85-92 and accompanying text.

most cybercrime undermines the reactive model's credibility as a way to address victimization in the cyber-world.

This article is, as was explained at its outset, a speculation. It is a conjecture on how principles of criminal law might be used to develop an alternative strategy that is based not on reacting to cybercrime, but on preventing it. It is exceedingly difficult to forecast how law may evolve. It is even more difficult to do so when the forecast involves the evolving assimilation of technologies which defy basic premises – e.g., identity, spatial constraints, or territorial authority – that have shaped criminal law as we know it. Notwithstanding these difficulties, it is imperative that we not content ourselves with "what has been," but endeavor, as best we can, to articulate strategies that are suitable for a phenomenon which has only recently emerged, but which, it is already clear, has the capacity to overwhelm law enforcement.

In the summer of 2003, a bank in Kearney, Nebraska was victimized by Malaysian hackers who stole debit card account access numbers.[410] The bank responded quickly and prevented major losses; according to a bank officer, the only effect its customers felt was "the inconvenience of getting new debit cards issued to them."[411] When asked if the bank intended to report the matter to law enforcement, the bank officer said it would not, since the matter would be handled internally.[412] The Kearney bank was very fortunate that its losses were so small; other U.S. banks and businesses have not been so fortunate. Assume, for the sake of analysis, that the Kearney bank *had* suffered substantial losses and that it identified the attacks as coming from Malaysia. In this scenario, such substantial losses would warrant calling in law

[410]*See, e.g., Counterfeit Ring Hacks Nebraska Bank's Computer*, USA TODAY, July 23, 2003, *available at* http://www.usatoday.com/tech/news/computersecurity/2003-07-23-ne-hack_x.htm (last visited September 30, 2004).

[411]*See id.*

[412]*See id.*

enforcement to apprehend the perpetrators. Assume, then, that in this hypothetical scenario, the President of the Kearney bank contacts local law enforcement. Kearney is a town of approximately 30,000 with a police force that has forty-eight regular officers.[413] Like most small police departments, the Kearney Police Department most likely does not have a cybercrime unit; if true, this would mean it would lack the expertise and resources needed to deal with the investigation of a crime of this type.[414]

Let us assume, however, that the Kearney Police Department can conduct a basic cybercrime investigation. The investigation indicates that the attack came from Malaysia, but that Malaysia may not be the actual source. To identify the actual source of the attack, the local police would have to be able to track the "path" taken by the attack, perhaps through a number of intervening computers, which is not an easy task. We will be generous, though, and assume they are able to do this and that they finally identify the attack as having come from Rio de Janeiro, Brazil. Although they have discovered the source of the attack, this information may not identify the attackers. To identify the attackers, they would likely need assistance from Brazilian authorities and Brazilian citizens, such as an Internet Service Provider; most local U.S. law enforcement officers are not familiar with the intricate processes required to obtain such assistance through formal channels.[415] Until recently, banks in Nebraska, Texas, and other U.S. states did not have to worry about off-shore attackers; now they do.

---

[413]*See, e.g.*, About Kearney, Living in Kearney, *available at* http://www.ci.kearney.ne.us/kearney.asp (last visited September 30, 2004); Police: Kearney/ Buffalo Law Enforcement Center, *available at* http://www.cityofkearney.org/index.asp?ID=7 (last visited September 30, 2004).

[414]*See, e.g.*, Susan W. Brenner & Joseph IV, *Transactional Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO L. 347, 375-77 (2002).

[415]*See id.*

Even if our hypothetical Kearney Cybercrime Squad is able to identify the appropriate processes and successfully initiate them, obtaining the evidence can take months, if not years; the attackers may well have left Brazil by then, putting them out of the reach of even the Brazilian authorities. Even if we continue our generosity and assume that the Kearney Cybercrime Squad obtains the assistance and evidence it needs to identify the attackers and has them extradited and brought to Kearney for trial, the police and the prosecutor(s) handling the case still face significant obstacles. They may need to bring witnesses in to authenticate evidence or to otherwise establish the case against the accused perpetrators, which can be an expensive task.[416] Indeed, the whole process of investigating a case such as this and preparing it for trial is expensive; the resources needed to pursue a case such as this are often far beyond what a small city or county can afford.[417] Even if a small city or county can somehow afford to fund the investigation and prosecution of one set of cyberattackers, it most certainly will not be able to repeat the process as attacks from off-shore perpetrators continue. Without a doubt, these attacks will continue; the United States is the richest country in the world and, as such, is an attractive victim for those who have learned how to use cyberspace to extort, steal and defraud (among other nefarious activities).

As this cautionary tale demonstrates, we cannot defend ourselves and our assets by reacting to attacks launched against us from cyberspace; despite what resources we have, we may never identify the architect of such an attack or the location from which it was launched. The traditional, reactive model of law enforcement is based on an assumed division of responsibility for maintaining order: The military maintains external order by discouraging and responding to hostile action by other nation-states, while law enforcement maintains internal

[416] *Id.*

[417] *Id.*

order by reacting to instances in which our citizens prey upon one another. This division of labor assumes a perimeter; that is, it assumes civilian law enforcement deals only with internal threats. Perimeters do not exist in cyberspace; cyberspace is permeable, and geography is irrelevant. The assumptions that shaped the reactive model do not hold in cyberspace, and we are well on our way to becoming defenseless unless we can devise an alternative model, one that can deal with the realities of cybercrime.

The model outlined in this article may well not be the appropriate alternative. It is offered as a step in the process of conceptualizing how we can defend ourselves against cybercrime without losing the benefits that this new experiential reality can confer.